UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

T.D., A.G., J.G., and K.W., *individually, and on behalf of all others similarly situated,* Plaintiffs, v. PIEDMONT HEALTHCARE, INC., Defendant.	Case No. 1:23-cv-05416-TWT **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs T.D., A.G., J.G., and K.W. (“Plaintiffs”),[1] patients of Piedmont Healthcare, Inc. (“Piedmont “or “Defendant”), bring this class action lawsuit against

[1] In order to avoid compounding the injuries and damages which give rise to this putative class action lawsuit and given the highly sensitive nature of the non-public, confidential and highly sensitive personal health information disclosed by Defendant without consent, Plaintiffs will move this Honorable Court for permission to proceed anonymously. *See, e.g.*, *Doe v. Archdiocese of Atlanta*, 328 Ga. App. 324, n. 20, 761 S.E.2d 864, 869 (2014).

PIEDMONT HEALTHCARE, INC. ("Piedmont" or "Defendant") in their individual capacities and on behalf of all others similarly situated and allege, upon personal knowledge as to their own actions and their counsel's investigation and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. This action arises from Piedmont's conscious decision to prioritize its desires for financial gain over its patients' privacy rights.

2. Plaintiffs bring this action on behalf of themselves and millions of other patients (collectively, the "Users") whose medical privacy was violated by Piedmont's use of Meta Platforms, Inc., d/b/a Meta's ("Meta" or "Facebook") tracking and collection tools.[2]

3. Plaintiffs are Piedmont patients who allege that Piedmont installed the Meta Collection Tools on its public website (https://www.piedmont.org/, the "Website") and its "Piedmont MyChart" patient portal (available at mychart.piedmont.org, "MyChart" or the "Patient Portal") (collectively, the "Web Properties") to share their confidential health information ("Private Information,"

[2] The Facebook tracking and collection tools include the Meta Pixel, Meta SDK, Meta Conversions API, customer list uploads, social plug-ins, the Meta Graph API, server-to-server transmissions and similar collection tools (collectively, "Meta Collection Tools").

including personally identifiable information ("PII") and protected health information ("PHI")) with Meta for financial gain in violation of federal and state laws.

4. Piedmont used these Meta Collection Tools to divulge the Private Information of Users of its Web Properties for marketing, re-marketing and analytics purposes despite its express promise that it: "Piedmont Providers may not use and disclose your PHI for marketing purposes except in limited circumstances as authorized by law or unless you have given us written authorization."[3]

5. The Private Information of potentially millions of active or potential patients of Piedmont's Web Properties was improperly and unlawfully disclosed to Facebook without their knowledge or consent. Piedmont did so because it knew that this sensitive information had tremendous value and that Plaintiffs and Class Members would ***not*** consent to the collection, disclosure and use of their Private Information if they were provided a choice or they would demand significant compensation for same.

6. Piedmont encouraged and/or required Plaintiffs and Class Members to use its Web Properties, including MyChart, to receive healthcare services, and

[3] *See* https://www.piedmont.org/media/file/PHC-Joint-Notice-Privacy-Practice.pdf (last accessed Jan. 11, 2024).

Defendant's Website and Patient Portal encourage and require patients to provide Private Information in order to facilitate healthcare treatment including, but not limited to, to search for a doctor, learn more about their conditions and treatments, access medical records and test results and manage appointments.

7. At all times that Plaintiffs and Class Members visited and utilized Defendant's Website and MyChart portal to receive medical services, they had a reasonable expectation of privacy that their Private Information would remain secure and protected and only utilized for medical purposes.

8. Further, Piedmont made expressed and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

9. Simply put, Piedmont broke those promises again and again.

10. The Facebook tracking pixel (the "Meta Pixel"), installed and configured by Defendant Piedmont, is a "piece of code" that allowed Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."[4] It also allowed Defendant to optimize the delivery of ads, measure

[4] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Jan. 12, 2024).

cross-device conversions, create custom advertising groups or "audiences," learn about the use of the Web Properties, and optimize advertising and marketing costs.[5]

11. Invisible to the naked eye, pixels—which are configured by the website owner, here, Piedmont—collect and transmit information from Users' browsers to unauthorized third parties including, but not limited to, Facebook.[6]

12. In particular, the Meta Pixel tracks visitors to the Web Properties and the actions they take as they interact with the website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box). [7]

[5] *Id.*

[6] The Meta Pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the Meta Pixel to a webpage is a multi-step process that must be undertaken by the website owner, namely, Piedmont.

[7] A pixel is a piece of code that "tracks the people and type of actions they take." RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jan. 11, 2024). Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Meta Pixel data to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients.

13. The use of tracking technologies, such as the Meta Pixel coincided with Piedmont's executive leadership giving free rein to a new Chief Marketing Officer ("CMO"), who emphasizes a focus on patient data and views patients' adoption of digital tools as a key measure of success.

14. The CMO, Mr. Bergsma, stated: "[w]hether people book online, whether they check-in before they walk-in, whether they open a MyChart account, which is literally your account where all your data sits – and all of those metrics are also at a record high." Mr. Bergsma continues, "[t]hat was important because our campaign and our brand positioning was mostly about us being distinct in the marketplace, because we'd had this digital transformation at Piedmont that most healthcare systems haven't yet adopted – or at least to the same level … **so we literally talked about adopting those tools in our campaign, and therefore, it was important that we measured them as well**."[8]

[8] *'Almost overwhelmed': How an ex-P&G US marketer ditched cohorts, personas, blended Ehrenberg-Bass, Binet & Field textbooks word for word, landed biggest marketing budget in $7bn company's history – and all KPIs are powering***,** https://www.mi-3.com.au/17-04-2023/how-ex-pg-us-marketer-ditched-cohorts-personas-and-restrictive-segmentation-blended-0 (last visited Jan. 9, 2024) (**Audio**: https://www.mi-3.com.au/17-04-2023/how-ex-pg-us-marketer-ditched-cohorts-personas-and-restrictive-segmentation-blended, timestamp 00:46:30-00:47:45 (last visited Jan. 9, 2024)).

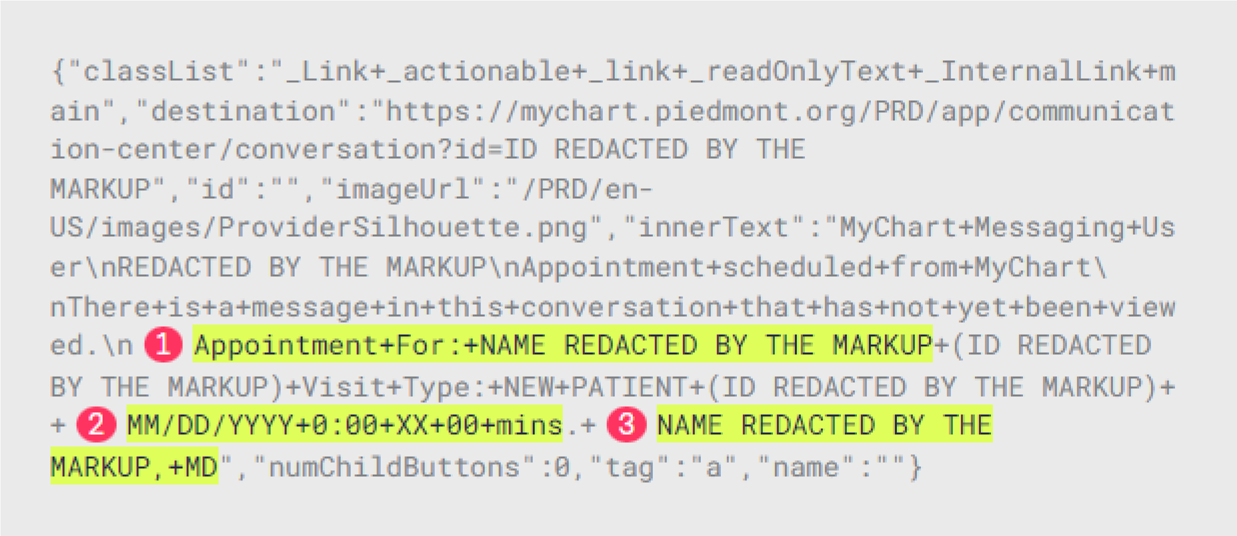
15. Piedmont intentionally installed the Meta Pixel on its Web Properties and configured the Meta Pixel to transmit and disclose Plaintiffs' and Class Members' Private Information to Facebook.

16. Piedmont's marketing campaign continued to break internal records and clipped onward unimpeded until, on June 16, 2022, Piedmont was named in an article titled *Facebook Is Receiving Sensitive Medical Information from Hospital Websites* published in the Markup, "a nonprofit newsroom that investigates how powerful institutions are using technology to change our society."[9]

17. The article concerned Piedmont's use of the Meta Pixel to send Facebook highly sensitive health information that it collected from patients within the MyChart portal, which "told Facebook the patient's name, the name of their doctor, and the time of their upcoming appointment."[10]

[9] *See* https://themarkup.org/about (stating that "[w]e are a new kind of media organization, staffed with an unparalleled roster of quantitative journalists who pursue meaningful, data-driven investigations").

[10] *See* https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last accessed Jan. 11, 2024).



```
{"classList":"_Link+_actionable+_link+_readOnlyText+_InternalLink+m
ain","destination":"https://mychart.piedmont.org/PRD/app/communicat
ion-center/conversation?id=ID REDACTED BY THE
MARKUP","id":"","imageUrl":"/PRD/en-
US/images/ProviderSilhouette.png","innerText":"MyChart+Messaging+Us
er\nREDACTED BY THE MARKUP\nAppointment+scheduled+from+MyChart\
nThere+is+a+message+in+this+conversation+that+has+not+yet+been+view
ed.\n 1 Appointment+For:+NAME REDACTED BY THE MARKUP+(ID REDACTED
BY THE MARKUP)+Visit+Type:+NEW+PATIENT+(ID REDACTED BY THE MARKUP)+
+ 2 MM/DD/YYYY+0:00+XX+00+mins.+ 3 NAME REDACTED BY THE
MARKUP,+MD","numChildButtons":0,"tag":"a","name":""}
```

Source: mychart.piedmont.org, Mozilla Rally

18. In fact, Piedmont shared the sensitive healthcare information of millions of patients with unauthorized third parties, including Facebook, for years prior to the release of The Markup's article, which tracks with Mr. Bergsma's boasts about Piedmont's adoption of "digital tools" as part of its new marketing campaign.[11]

19. Operating as designed, Defendant's tracking Meta Pixel allowed the Private Information that Plaintiffs and Class Members submitted to Piedmont to be unlawfully disclosed to Facebook.

[11] Shortly after the article was published, Piedmont removed the Pixel from its Web Properties. By January 2023, however, Piedmont had reinstalled the Pixel on its Web Properties and continued to use it for a yet-undetermined amount of time.

20. For example, when a patient used Piedmont's Web Properties, the Meta Collection Tools directed Plaintiffs' or Class Members' browser to send a message to Facebook's servers, those messages transmitted the content of their communications to Meta, including, but not limited to: (1) signing-up for the Patient Portal; (2) signing-in or -out of the Patient Portal; (3) taking actions inside the Patient Portal; (4) making, scheduling, or participating in appointments; (5) upon information and belief, exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; (6) conduct a search on Piedmont's Web Properties and (7) other information that qualifies as "protected health information" under federal and state laws.

21. The information transmitted from Piedmont's Web Properties to Meta includes information sufficient to identify a specific patient under federal law (such as IP address information, device identifiers, and advertising identifiers that Meta associates with a patient's Meta account), and may also include a patient's demographic information, email address, phone number, computer ID address or contact information entered as emergency contacts or for advanced care planning, along with information like appointment type and date, a selected physician, button

and menu selections, the content of buttons clicked and typed into text boxes, and information about the substance, purport, and meaning of patient requests for information from Piedmont under federal and state health privacy laws.

22. Among the personally identifying information that Defendant discloses is the User's unique and persistent Facebook ID ("Facebook ID" or "FID") which allows Facebook and other third parties to personally identify that User and associates the Users' Private Information with its Facebook profile. The Facebook ID is a string of numbers Facebook uses to identify and connect to a User's Facebook profile. Facebook creates a Facebook ID automatically, whether or not you choose to create a username.[12] Thus Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it.

23. Transmitting the Private Information allowed a third party (*e.g.*, Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy or AIDS.

[12] *See* https://www.facebook.com/help/211813265517027 (last visited Jan 10. 2024).

24. Meta collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users allowing Piedmont to target advertisements both on and off Facebook. For example, Piedmont and Meta can target ads to a person who has used the Website or the Patient Portal and exchanged communications about a specific condition, such as cancer.

25. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996) and Georgia law relating to the confidentiality of medical records, O.C.G.A. §§ 31-33-2, 31-33-8, both prohibit healthcare providers from sharing health care information, medical records and related information with third parties except as needed for a patient's treatment, payment or with their consent. Importantly, these laws give patients a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment, because this information may not be disclosed outside the healthcare setting without notice and consent.

26. The United States Department of Health and Human Services ("HHS") recently confirmed that HIPAA and its regulations prohibit the transmittal of individually identifiable health information by tracking technology like the Meta

Pixel without the patient's authorization and other protections like a business associate agreement with the recipient of patient data.[13]

27. Reiterating the importance of and necessity for data security and privacy concerning health information, the Federal Trade Commission ("FTC") recently published a bulletin entitled *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, in which it noted that:

> [h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information.***[14]

[13] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

[14]*See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), available at https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Jan. 11, 2024).

28. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***<u>But when companies use consumers’ sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.</u>***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***<u>may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers’ affirmative express consent for the disclosure of sensitive health information</u>***.[15]

29. Not only did Piedmont willfully and intentionally incorporate the tracking Meta Pixel into its Web Properties, but it also never disclosed to Plaintiffs

[15] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers’ authorization.

or Class Members that it shared their sensitive and confidential communications via the Web Properties with Facebook.

30. As a result, Plaintiffs and Class Members were unaware that their PII and PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare providers, looked up their conditions and/or treatments, and logged into the MyChart portal.[16]

31. The full extent of Piedmont's unlawful disclosures is not yet known, but the numbers may be staggering. According to Piedmont's website, "[m]illions of patients conveniently engage with Piedmont online, ***as they visited Piedmont.org***

[16] In contrast to Defendant, in recent months several healthcare providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g., Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Jan. 12, 2023); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Jan. 12, 2024); *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

***and Piedmont MyChart over 30 million times, scheduled more than 515,000 online appointments and over 154,000 virtual visits*.”[17]

32. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiffs’ and Class Members’ communications and medical information safe, secure and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

33. Piedmont, however, failed in its obligations and promises by utilizing the Meta Collection Tools on its Web Properties, knowing that such technology would transmit and share Plaintiffs’ and Class Members’ Private Information with unauthorized third parties. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure their Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users’

[17] https://www.piedmont.org/about-piedmont-healthcare/about-us-home (emphasis added) (the cited quote was obtained when this webpage was accessed on October 16, 2023; as of January 9, 2024, Piedmont removed its boast that patients had accessed the Web Properties over 30 million times).

information; (iii) failing to obtain the consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the Meta Pixel or any other other tracking technologies; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design, and monitor its Web Properties in order to maintain the confidentiality and integrity of patient Private Information.

34. Piedmont's interception, dissemination, and use of Private Information not only violates federal and state law but also harms patients by intruding upon their privacy; erodes the confidential nature of the provider-patient relationship; and takes patients' property and property rights without compensation and ignores their right to control the dissemination of their health information to third parties.[18] In addition, Piedmont has been unjustly enriched by its misconduct, obtaining unearned revenues derived from the enhanced advertising services and more cost-efficient marketing on Facebook it receives in exchange for its unauthorized disclosure of patient information.

[18] It is unknown without discovery whether the Private Information was further disseminated to additional third-party marketing companies (*e.g.*, Google, Twitter, Bing, LinkedIn, HotJar, LifePerson, The Trade Desk, or Adobe) for the purposes of building profiles and retargeting or to insurance companies to set rates.

35. Plaintiffs seeks to remedy these harms for themselves and the millions of similarly affected persons, and therefore bring causes of action for (1) Invasion of Privacy; (2) Breach of Fiduciary Duty; (3) Negligence; (4) Breach of Implied Contract; (5) Breach of Contract; (6) Unjust Enrichment; and (7) Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq.*

PARTIES

36. Plaintiffs T.D. is a natural person and citizen of Georgia, and he resides in DeKalb County.

37. Plaintiffs A.G. is a natural person and citizen of Georgia, and he resides in DeKalb County.

38. Plaintiffs J.G. is a natural person and citizen of Georgia, and she resides in DeKalb County.

39. Plaintiffs K.W. is a natural person and citizen of Georgia, and he resides in DeKalb County.

40. Defendant Piedmont Healthcare, Inc. is a Georgia company with its principal place of business at 800 Howell Mill Road, Suite 850, Atlanta, GA, 30318. Defendant is a Georgia-wide integrated network of physician clinics, outpatient centers and hospitals. Its network consists of more than 23 hospitals, 12,000 doctors, 65 urgent care centers, and 1,900 clinics.

41. Headquartered in Atlanta, Piedmont is the largest healthcare provider in the state of Georgia. Defendant advertises that it is committed to "empowering our patients through great care," serving more than 3.7 million patients annually.

42. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 "HIPAA").

JURISDICTION & VENUE

43. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under federal law, including the Electronic Communications Privacy Act ("ECPA"), 28 U.S.C. § 2511, *et seq.*

44. The Court has supplemental jurisdiction over Plaintiffs' claims arising under state law under 28 U.S.C. § 1367.

45. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the class is a citizen of a state different from Defendant.

46. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and a substantial portion of the acts and

omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

47. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this district and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this district.

PROCEDURAL BACKGROUND

48. This case was originally filed on October 25, 2023, in the Superior Court of Fulton County.

49. On November 27, 2023, Defendant filed a Notice of Removal (ECF No. 1) removing this matter from the Superior Court of Fulton County, Georgia to the Northern District of Georgia, Atlanta Division.

FACTUAL BACKGROUND

I. PIEDMONT REQUIRED THE COLLECTION OF PLAINTIFFS' PRIVATE INFORMATION.

50. Throughout the Class Period, Piedmont maintained and operated the Web Properties, by and through which Piedmont encouraged and/or required patients to seek healthcare services.

51. To obtain healthcare services through the Web Properties, Plaintiffs and other Class Members were required to provide their PHI and PII to Piedmont.

52. On information and good faith belief, each step of this process was

tracked and logged by the Meta Pixel.

53. On information and good faith belief, throughout the Class Period, the process for obtaining healthcare services on the Web Properties has been substantially the same in all material respects throughout the United States.

II. PIEDMONT SECRETLY DISCLOSED & PERMITTED THIRD PARTIES TO INTERCEPT PLAINTIFFS' & CLASS MEMBERS' PHI.

54. Completely unbeknownst to Plaintiffs and other Class Members, and continuing to at least June 2022, Private Information that they communicated to Piedmont through the Website while obtaining healthcare services was disclosed to Meta.

A. Piedmont Improperly Disclosed Plaintiffs' & Class Members' Private Information.

55. In approximately 2020, Piedmont launched a marketing campaign to connect Plaintiffs and Class Members to Defendant's digital healthcare platform with the goal of increasing revenue.

56. To accomplish this, Piedmont utilized Facebook advertisements and intentionally installed the Meta Pixel on its Web Properties.

57. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare Partners. Meta defines its Partners to include businesses that use

Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

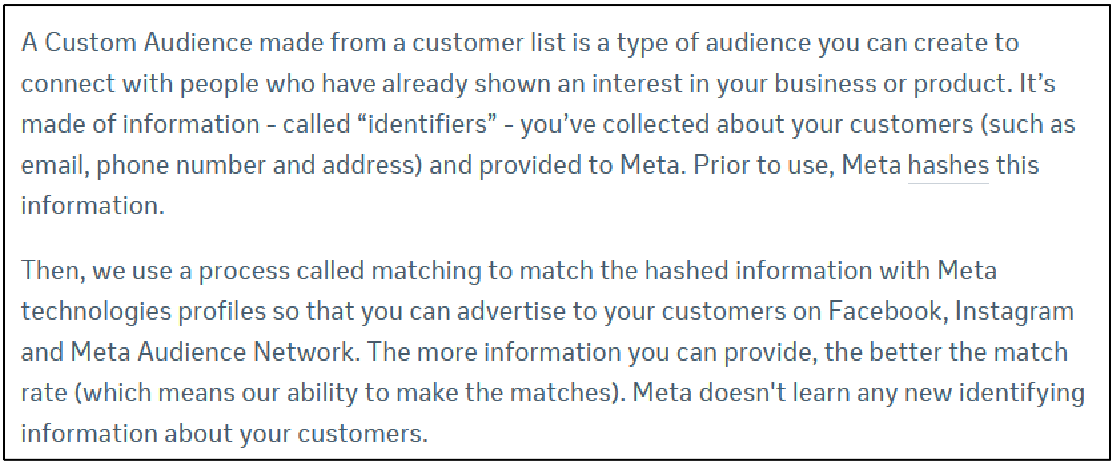
58. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.[19]

59. Meta offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Meta healthcare Partner's website embedded with the Meta Pixel, the Meta Pixel will be triggered to send Meta "Event" data that Meta matches to its Users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Meta Pixel can then be used to measure the effectiveness of an advertising campaign.[20]

[19] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*.

[20] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), *https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d*

60. Meta also allows Meta healthcare Partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[21]



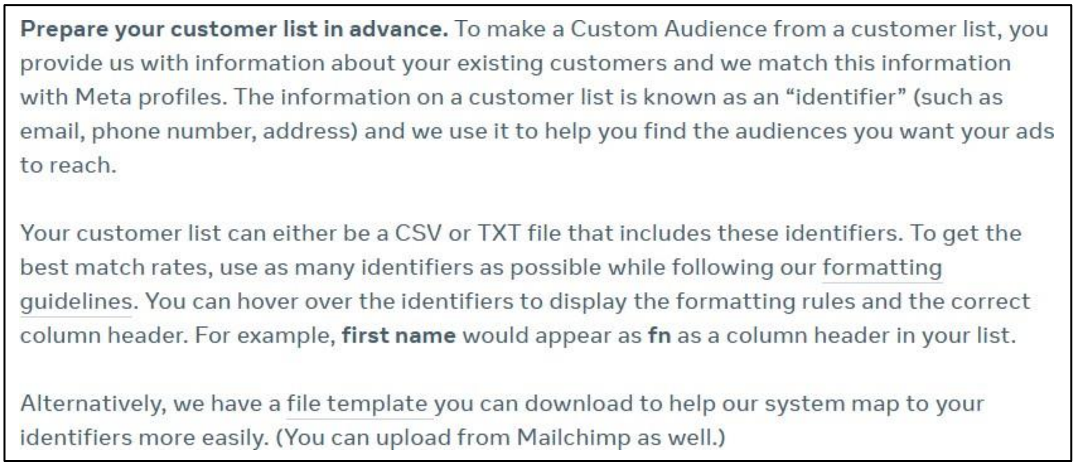
A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.

Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

61. Meta provides detailed instructions for healthcare Partners to send their patients' individually identifiable information to Meta through the customer list upload. For example:

_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa

[21] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*.



Prepare your customer list in advance. To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.

Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.

Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

62. Meta healthcare Partners can then use the Custom Audiences derived from their patient list with the Meta Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

63. Without discovery, Plaintiffs do not yet know whether Piedmont uploaded patient lists to Meta. However, Plaintiffs do know that when they and Class Members sought and used Defendant's services as a medical provider, and utilized the Web Properties services, including My Chart, their Private Information was intercepted in real time and then disseminated to Facebook, and potentially to other third parties, via the Meta Pixel and other Meta Collection Tools that Defendant secretly installed on its Web Properties.

64. According to Piedmont's own statements on the Website, as of October 2023, Users had visited Piedmont's Web Properties over 30 million times and claimed to have over 3.7 million annual patients. [22]

65. Plaintiffs and Class Members did not intend or have any reason to suspect their Private Information would be shared with Facebook or that Defendant was tracking their every movement and disclosing same to Facebook when they entered highly sensitive information on Defendant's Website and Patient Portal.

66. Defendant did not disclose to or warn Plaintiffs or Class Members that Defendant used Plaintiffs' and Class Members' Web Properties submissions for Facebook's marketing purposes.

67. Defendant installed the Meta Pixel used to disclose Plaintiffs' and Class Members' Private Information via the Meta Pixel from at least December 2018, or earlier, to approximately June 17, 2022. The Markup published its article about Piedmont's use of the Meta Pixel, and Piedmont then removed the Meta Pixel from its Web Properties. By January 2023, however, Piedmont had reinstalled the Meta

[22] https://www.piedmont.org/about-piedmont-healthcare/about-us-home (emphasis added) (after filing this lawsuit, Piedmont removed its boast that patients had accessed the Web Properties over 30 million times).

Pixel on its Web Properties and continued to use them for a yet-undetermined amount of time.

68. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Meta.

69. Defendant's unauthorized disclosure is not just limited to activity on the public Website, but the disclosure also involved information contained within the highly sensitive and private MyChart portal, which requires patients to provide a specific login.

70. Piedmont disclosed to Meta the following non-public private information:

a. when a patient clicks to register for the Patient Portal;

b. information that a patient types into registration forms;

c. when a patient clicks to log in to the Patient Portal;

d. when a patient sets up or schedules an appointment;

e. information that a patient types into an appointment form;

f. when a patient clicks a button to call the provider from a mobile device directly from the Website;

g. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

h. the communications a patient exchanges through Piedmont's Web Properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including whether they are made while a patient is still logged in to the Patient Portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged into the Patient Portal; and

i. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

71. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e. Meta Pixels) that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Meta—an unauthorized third party; and (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

B. *Meta's Collection Tools Redirect Patients' Data from Piedmont's Web Properties to Facebook to Use for Ad Targeting*

72. Facebook operates the world's largest social media company and generated nearly $117 billion in revenue in 2022, roughly 97% of which came from selling targeted advertising. [23]

73. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses, cookies, device identifiers, and advertising ID identifiers.

74. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code, such as the Meta Pixel.

75. Facebook then sells advertising space by highlighting its ability to target users.[24] Facebook can target users so effectively because it surveils user activity both on and off its site.[25] This allows Facebook to make inferences about

[23] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2022 RESULTS, https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx (last visited Jan. 12, 2024).

[24] WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Jan. 12, 2024).

[25] ABOUT FACEBOOK PIXEL,

users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”[26]

76. Facebook compiles this information into a generalized dataset called “Core Audiences,” which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[27]

77. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

78. Advertisers can also build “Custom Audiences.”[28] Custom Audiences enable advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”[29]

https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Jan. 12, 2024).

[26] AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Jan. 12, 2024).

[27] EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Jan. 12, 2024).

[28] ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Jan. 12, 2024).

[29] AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Jan. 12, 2024).

79. With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[30]

80. Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences *only if they first supply Facebook with the underlying data*. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[31]

81. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and

[30] ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Jan. 12, 2024).

[31] CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Jan. 12, 2024).

better reach and serve people who might be interested in their products and services."[32]

82. Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

83. The Business Tools are automatically configured to capture certain data, like when a User visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[33]

84. Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what

[32] THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Jan. 12, 2024).

[33] *See* FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 12, 2024).

content a visitor views or purchases.[34] Advertisers can even create their own tracking parameters by building a "custom event." [35]

85. One such Business Tool is the Meta Pixel. Facebook offers this code to advertisers, like Defendant, to integrate into their website. As the name implies, the Meta Pixel "tracks the people and type of actions they take."[36]

86. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[37]

87. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

[34] SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Jan. 12, 2024).

[35] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (last visited Jan. 12, 2024),

[36] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jan. 11, 2024).

[37] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

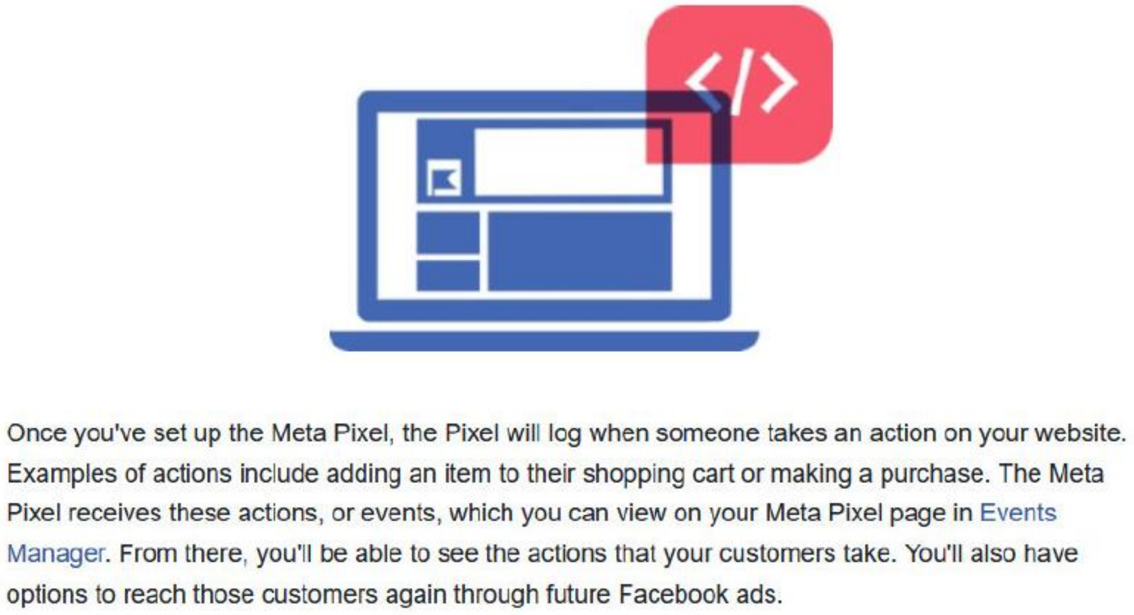
a. "measure cross-device conversions" and "understand how your cross-device ads help influence conversion.";

b. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

c. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[38]

88. Meta explains that the Meta Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

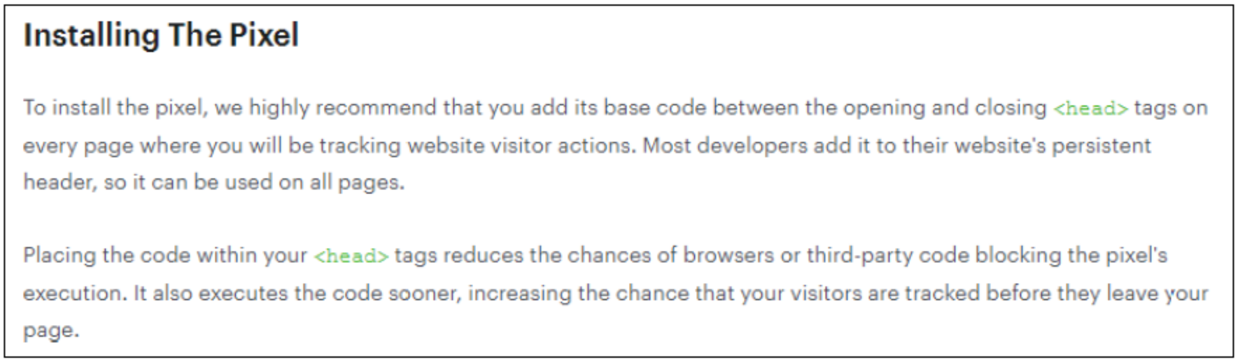
[38] *Id.*



Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

89. The Meta Pixel is customizable. Meaning, web developers can choose the actions the Pixel will track and measure.

90. Meta advises web developers to place the Meta Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:



Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your <head> tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

91. Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.[39]

92. If a healthcare provider, such as Piedmont, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her healthcare provider—traveling directly from the user's browser to Facebook's server.

93. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

94. This contemporaneous, and secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by the Facebook code installed by Defendant and concurrent with the Users' communications with the host website.

[39] Meta, Meta Pixel (2023), https://www.facebook.com/business/tools/meta-pixel.

Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code, and the Facebook code Defendant embedded.

95. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing."[40]

96. Piedmont, through its installation and use of the Meta Pixel, disclosed to Meta the content of patient communications while its patients were exchanging communications with Piedmont's Web Properties.

97. Piedmont's CMO, Mr. Bergsma, recently bragged on a podcast about how Piedmont changed its marketing strategy in conjunction with its "digital transformation" and began targeting markets based on individuals' health conditions. Mr. Bergsma stated:

> We got rid of the defined personas – the busy soccer mom and the elderly single person and the young starter. Now we actually apply a very broad media buy, with the exception of some ethnic groups like African Americans or Hispanics, in order to reach those areas in the state of Georgia where we have a very large multicultural population.

[40] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA Today (March 4, 2020 4:52 am), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/#.

> . . .
>
> Instead of using personas, ***we define the market as 'the market for cancer', or 'the market for heart patients', or 'the market for neuro patients'.*** We have broad application, rather than staying within the neuro patient market, we're looking at A, B and C segments and adjusting our media to it. So we've gotten more exact and more precise in defining what segment we're after from a service perspective, less from a consumer sociodemographic perspective.[41]

98. While Mr. Bergsma did not mention the words "Custom Audiences" in this interview, Piedmont's use of the Meta Pixel to send Facebook the names of patients' doctors would have permitted Piedmont to specifically target its existing patients with Facebook ads *based on their health conditions*, as well as create Lookalike Audiences for the same purpose. This could only be accomplished by Piedmont disclosing to Meta the content of those patients' communications on Piedmont's Web Properties, providing Facebook with a list of Piedmont's patients,

[41] *'Almost overwhelmed': How an ex-P&G US marketer ditched cohorts, personas, blended Ehrenberg-Bass, Binet & Field textbooks word for word, landed biggest marketing budget in $7bn company's history – and all KPIs are powering*, https://www.mi-3.com.au/17-04-2023/how-ex-pg-us-marketer-ditched-cohorts-personas-and-restrictive-segmentation-blended-0 (last visited Jan. 9, 2024) (**Audio**: https://www.mi-3.com.au/17-04-2023/how-ex-pg-us-marketer-ditched-cohorts-personas-and-restrictive-segmentation-blended, timestamp 00:09:15-00:10:50 (last visited Jan. 9, 2024)).

or otherwise disclosing the identity of Piedmont's patients to Meta through the Meta Collection Tools.

C. Defendant's Use of Source Code, the Meta Pixel & Interception of HTTP Requests.

99. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet, or smartphone) accesses web content through a web browser (e.g., Google's Chrome, Mozilla's Firefox, Apple's Safari, and Microsoft's Edge).

100. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via web browsers.

101. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be

communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. [42]

102. A patient's HTTP Request essentially asks the Website to retrieve certain information (such as the name of a doctor with whom a patient makes an appointment), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate the Web Properties).

103. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

104. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the

[42] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

background without notifying the web browser's user. The Meta Pixel and other tracking technologies Piedmont uses constitute source code that does just that. These tracking technologies thus act much like a traditional wiretap.

105. Piedmont encourages customers to use its Web Properties to obtain healthcare services, such as making appointments with doctors and other providers, and take other actions related to their personal health care. When interacting with Piedmont's Web Properties like this, Plaintiffs and Class Members convey highly private and sensitive information to Piedmont.

106. When patients visit Piedmont's Web Properties via an HTTP Request to Piedmont's server, that server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code, including Piedmont's Meta Pixel.

107. Thus, Piedmont, is in essence, handing patients a tapped device, and once the webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Web Properties to trigger the tap, which intercepts those communications intended only for Piedmont and transmits those communications to third parties, including Facebook.

108. Defendant intentionally configured the Meta Pixel installed on its Web Properties to capture both the "characteristics" of individual patients'

communications with the Defendant's Web Properties (e.g., their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

109. Without any action or authorization, Defendant commands Plaintiffs' and Class Members' computing devices to contemporaneously re-direct the Plaintiffs' and Class Members' identifiers and the contents of their communications to Facebook.

D. Meta Uses Identifiers to Match The Health Information It Collects With Facebook Users.

110. Meta uses cookies to identify patients, including cookies named c_user, datr, fr, and _fbp.

111. The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Meta uses the c_user cookie to record user activities and communications.

112. An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting "View page source," (4) executing a control-f function

for “UserID,” and (5) copying the number value that appears after “UserID” in the page source code of the Facebook user’s page.

113. Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing www.facebook.com/4 into a browser and hitting enter, a browser directs to Mr. Zuckerberg’s page at www.facebook.com/zuck.

114. A user’s Facebook ID is therefore linked to their Facebook profile, which contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user’s Facebook ID uniquely identifies an individual’s Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user’s corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

115. The Meta datr cookie identifies the web browser the patient is using. It is an identifier unique to each patient’s specific web browser, so it is another way Meta can identify Facebook users.

116. Meta keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies

associated with his or her Facebook account from Meta by using the Facebook "Download Your Information" tool.

117. The Meta fr cookie is an encrypted combination of the c_user and datr cookies.[43]

118. The c_user, datar, and fr cookies are traditional third-party cookies, meaning they are cookies associated with a party other than the entity with which a person is communicating at the time. In the case of Piedmont, they are third-party cookies because Meta is a third party to the communication between a patient and their healthcare provider.

119. The Meta _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the healthcare provider using the Meta Pixel. (The letters fbp are an acronym for Facebook Pixel.)

120. The _fbp (or Facebook Pixel) cookie is also a third-party cookie in that it is also a cookie associated with Meta that is used by Meta to associate information about a person and their communications with non-Meta entities while the person is on a non-Meta website or application.

[43] *See* Gunes Acar, *et al.*, Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission (Mar. 27, 2015), https://securehomes.esat.kuleuven.be/~ gacar/fb_tracking/fb_pluginsv1.0.pdf.

121. Meta disguises the _fbp cookie as a first-party cookie even though it is Meta's cookie on non-Meta websites.

122. By disguising the _fbp cookie as a first-party cookie for a healthcare provider rather than a third-party cookie associated with Facebook, Meta ensures that the _fbp cookie is placed on the computing device of patients who seek to access the patient portal.

123. Healthcare providers with a patient portal require patients to enable first-party cookies to gain access to their patient records through the portal.

124. The purpose of these portal-associated first-party cookies is security. The _fbp cookie is then used as a unique identifier for that patient by Meta. If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted—even though it is a Meta cookie—again, because Meta has disguised it as a first-party cookie. Meta also uses IP address and user-agent information to match the health information it collects from Meta healthcare Partners with Facebook users.

125. Accordingly, Defendant's Web Properties through the Meta Pixel and other tracking technologies routinely provide Facebook with Defendant's patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Web Properties, including not only their medical searches,

treatment requests, and the webpages they view, but also their name, email address, or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[44] Plaintiffs' and Class Members' identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

126. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

127. While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent Facebook from reading, understanding, and using the data.[45] In fact,

[44] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 12, 2024).

[45] *See* https://www.facebook.com/business/help/112061095610075?id=2469097953376494;

Facebook explicitly uses the hashed information it gathers to link Pixel-transmitted data to Facebook profiles.[46] Indeed, there would be no value in targeting Facebook users with Defendant's ads if Facebook couldn't read the hashed data it received from Defendant to know *who* to target.

128. As Facebook explains, "[a]utomatic advanced matching will tell your pixel to look for recognizable form fields and other sources on your website that contain information such as first name, last name and email address. The Meta Pixel receives that information along with the event, or action, that took place. This information gets hashed in the visitor's browser. ***We can then use the hashed information to more accurately determine which people took action in response to your ad***."[47] Similarly, Facebook tells businesses: "When you upload your customer list in Ads Manager to create a Custom Audience, the information in your list is hashed before it's sent to Facebook. ***Facebook uses this hashed information and compares it to our own hashed information. Then, we help build your audience by***

https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142

[46] *See* https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[47] https://www.facebook.com/business/help/611774685654668?id=12053%2076682832142

finding the Facebook profiles that match and create a Custom Audience for you from those matches."[48]

129. In other words, Facebook uses its own secret language to encode and then read and match individuals' information.

130. Facebook claims that after hashing individuals' Private Information (including their personal identifiers and PHI shared by Defendant) and matching it to Facebook profiles to create Custom Audiences, Facebook deletes the hashed data. Even assuming this is true, by that point, the damage is done—Facebook has read, understood, analyzed, and expressly taken action to match the shared PHI with specific individuals, with the express purpose of targeting those individuals with ads based on the data (PHI) that was shared and used to create Defendant's Custom Audiences—all at Defendant's request.

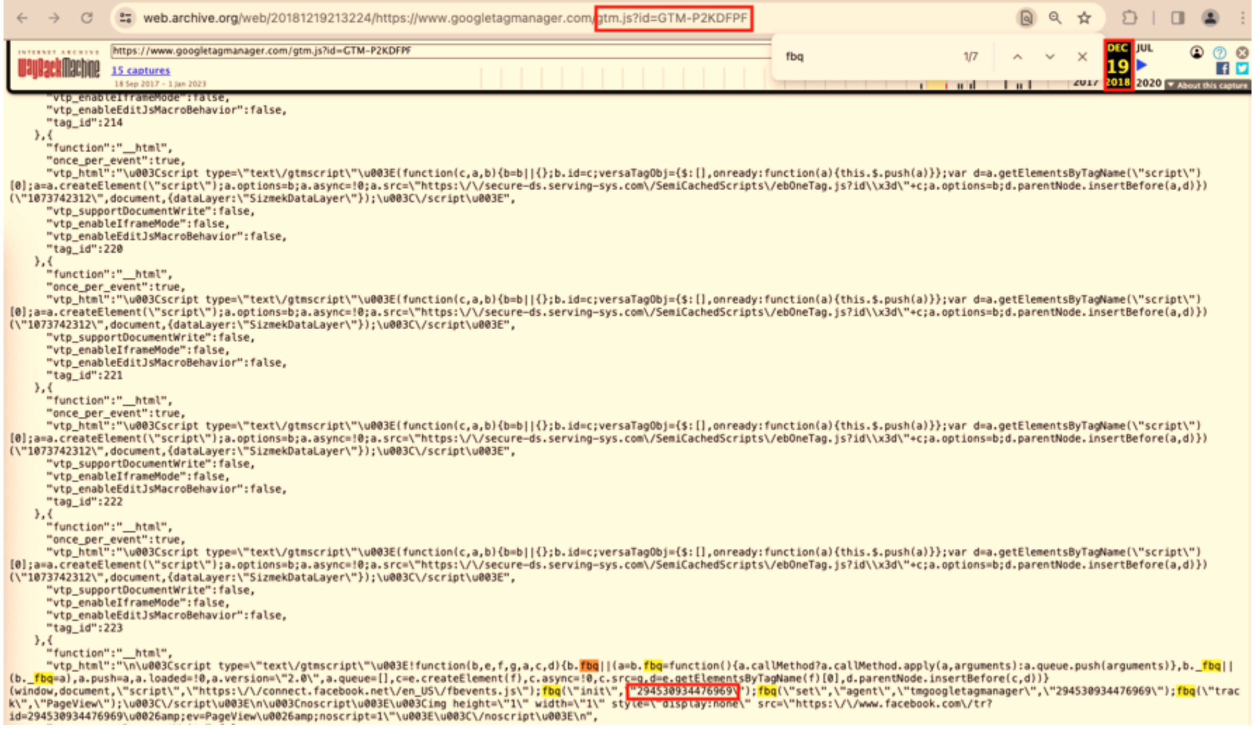
131. This disclosed PHI and PII allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with

[48] https://www.facebook.com/business/help/112061095610075?id=2469097953376494

Defendant's ads, Facebook also then sells that information to marketers who will online target Plaintiffs and Class Members.

E. Evidence that Piedmont Installed the Meta Pixel on its Web Properties and Used the Meta Pixel to Transmit Private Information to Meta.

132. An archive of a Google Tag Manager ("GTM1") on Piedmont's Web Properties dated December 19, 2018, shows the installation of the Meta Pixel with ID 294530934476969 ("Pixel1"):


web.archive.org/web/20181219213224/https://www.googletagmanager.com/gtm.js?id=GTM-P2KDFPF
INTERNET ARCHIVE
WaybackMachine
https://www.googletagmanager.com/gtm.js?id=GTM-P2KDFPF
15 captures
18 Sep 2017 - 1 Jan 2023
fbq
1/7
DEC
19
2018
JUL
2017
2020
About this capture

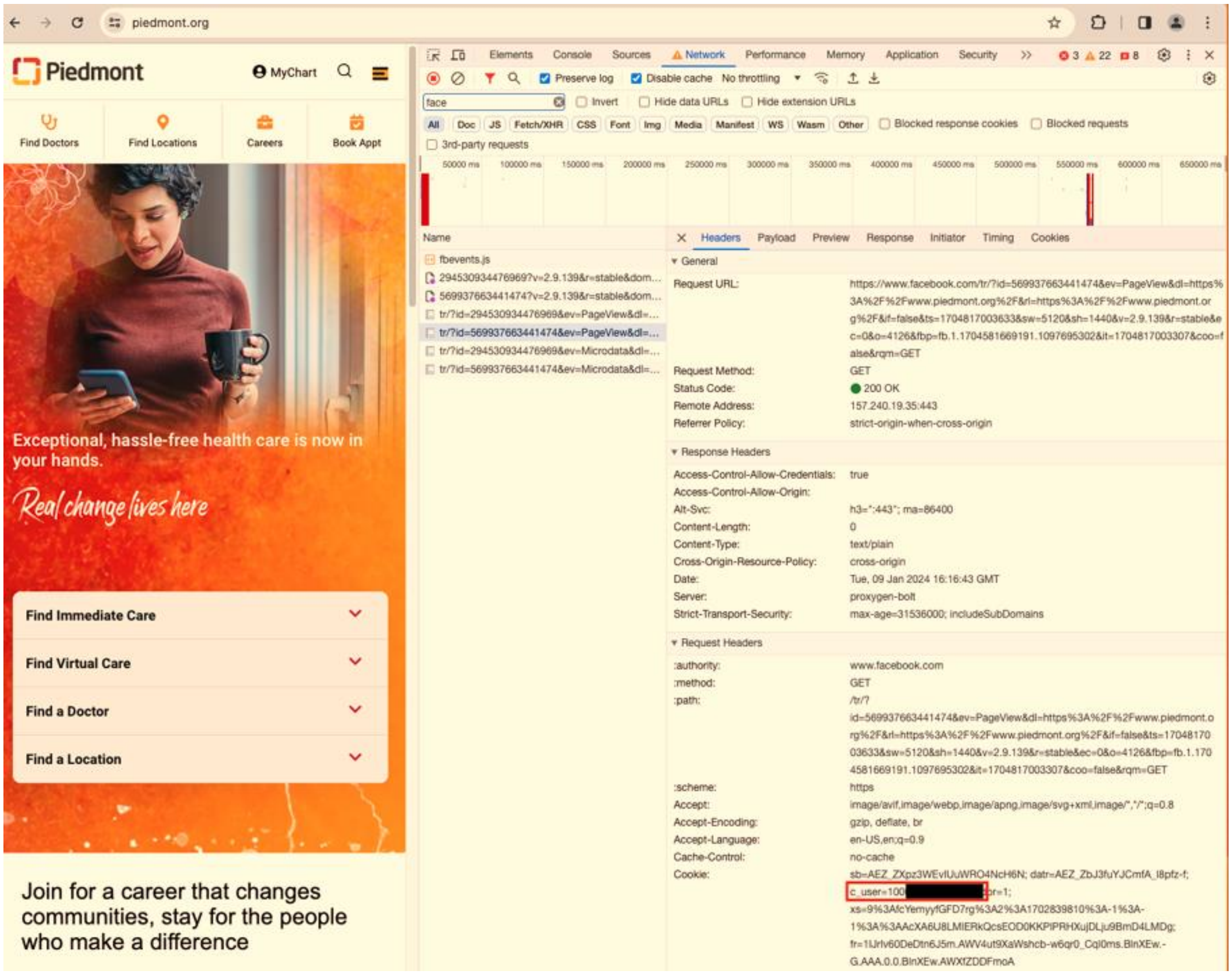
```
        "vtp_enableIframeMode":false,
        "vtp_enableEditJsMacroBehavior":false,
        "tag_id":214
    },{
        "function":"__html",
        "once_per_event":true,
        "vtp_html":"\u003Cscript type=\"text\/gtmscript\"\u003E(function(c,a,b){b=b||{};b.id=c;versaTagObj={$:[],onready:function(a){this.$.push(a)}};var d=a.getElementsByTagName(\"script\")
[0];a=a.createElement(\"script\");a.options=b;a.async=!0;a.src=\"https:\/\/secure-ds.serving-sys.com\/SemiCachedScripts\/ebOneTag.js?id\\x3d\"+c;a.options=b;d.parentNode.insertBefore(a,d)})
(\"1073742312\",document,{dataLayer:\"SizmekDataLayer\"});\u003C\/script\u003E",
        "vtp_supportDocumentWrite":false,
        "vtp_enableIframeMode":false,
        "vtp_enableEditJsMacroBehavior":false,
        "tag_id":220
    },{
        "function":"__html",
        "once_per_event":true,
        "vtp_html":"\u003Cscript type=\"text\/gtmscript\"\u003E(function(c,a,b){b=b||{};b.id=c;versaTagObj={$:[],onready:function(a){this.$.push(a)}};var d=a.getElementsByTagName(\"script\")
[0];a=a.createElement(\"script\");a.options=b;a.async=!0;a.src=\"https:\/\/secure-ds.serving-sys.com\/SemiCachedScripts\/ebOneTag.js?id\\x3d\"+c;a.options=b;d.parentNode.insertBefore(a,d)})
(\"1073742312\",document,{dataLayer:\"SizmekDataLayer\"});\u003C\/script\u003E",
        "vtp_supportDocumentWrite":false,
        "vtp_enableIframeMode":false,
        "vtp_enableEditJsMacroBehavior":false,
        "tag_id":221
    },{
        "function":"__html",
        "once_per_event":true,
        "vtp_html":"\u003Cscript type=\"text\/gtmscript\"\u003E(function(c,a,b){b=b||{};b.id=c;versaTagObj={$:[],onready:function(a){this.$.push(a)}};var d=a.getElementsByTagName(\"script\")
[0];a=a.createElement(\"script\");a.options=b;a.async=!0;a.src=\"https:\/\/secure-ds.serving-sys.com\/SemiCachedScripts\/ebOneTag.js?id\\x3d\"+c;a.options=b;d.parentNode.insertBefore(a,d)})
(\"1073742312\",document,{dataLayer:\"SizmekDataLayer\"});\u003C\/script\u003E",
        "vtp_supportDocumentWrite":false,
        "vtp_enableIframeMode":false,
        "vtp_enableEditJsMacroBehavior":false,
        "tag_id":222
    },{
        "function":"__html",
        "once_per_event":true,
        "vtp_html":"\u003Cscript type=\"text\/gtmscript\"\u003E(function(c,a,b){b=b||{};b.id=c;versaTagObj={$:[],onready:function(a){this.$.push(a)}};var d=a.getElementsByTagName(\"script\")
[0];a=a.createElement(\"script\");a.options=b;a.async=!0;a.src=\"https:\/\/secure-ds.serving-sys.com\/SemiCachedScripts\/ebOneTag.js?id\\x3d\"+c;a.options=b;d.parentNode.insertBefore(a,d)})
(\"1073742312\",document,{dataLayer:\"SizmekDataLayer\"});\u003C\/script\u003E",
        "vtp_supportDocumentWrite":false,
        "vtp_enableIframeMode":false,
        "vtp_enableEditJsMacroBehavior":false,
        "tag_id":223
    },{
        "function":"__html",
        "vtp_html":"\n\u003Cscript type=\"text\/gtmscript\"\u003E!function(b,e,f,g,a,c,d){b.fbq||(a=b.fbq=function(){a.callMethod?a.callMethod.apply(a,arguments):a.queue.push(arguments)},b._fbq||
(b._fbq=a),a.push=a,a.loaded=!0,a.version=\"2.0\",a.queue=[],c=e.createElement(f),c.async=!0,c.src=g,d=e.getElementsByTagName(f)[0],d.parentNode.insertBefore(c,d))}
(window,document,\"script\",\"https:\/\/connect.facebook.net\/en_US\/fbevents.js\");fbq(\"init\",\"294530934476969\");fbq(\"set\",\"agent\",\"tmgoogletagmanager\",\"294530934476969\");fbq(\"trac
k\",\"PageView\");\u003C\/script\u003E\n\u003Cnoscript\u003E\u003Cimg height=\"1\" width=\"1\" style=\"display:none\" src=\"https:\/\/www.facebook.com\/tr?
id=294530934476969\u0026amp;ev=PageView\u0026amp;noscript=1\"\u003E\u003C\/noscript\u003E\n",
```

133. The most recent archive of GTM1, dated January 1, 2023, shows two other Meta Pixels installed, with IDs 569937663441474 ("Pixel2") and 559505115631388 ("Pixel3").

134. Archives of GTM1's, Pixel1's, and Pixel2's configuration files demonstrate the actions that Piedmont took using the Meta Pixels that it installed and the custom events that it set up to transmit patients' Private Information to Meta.

135. Using the Pixels installed on its Web Properties, Piedmont transmitted PageView, Microdata, and SubscribedButtonClick events about Users' activities. Upon a user's arrival on Piedmont's homepage, Piedmont immediately sent a pair of PageView and Microdata events to Facebook revealing that the user was on the page, "https://www.piedmont.org/." As Users navigated beyond the homepage, Piedmont continued to disclose user data including Users': (i) physician search activities; (ii) keyword search activities (iii) appointment activities; and (iv) MyChart and bill payment activities.

136. In each of the transmitted Meta Pixel events, Piedmont included the "c_user" cookie, which Facebook uses to identify Users:



Exceptional, hassle-free health care is now in your hands.

Join for a career that changes communities, stay for the people who make a difference

face ☐ Invert ☐ Hide data URLs ☐ Hide extension URLs

☑ Preserve log ☑ Disable cache

☐ Blocked response cookies ☐ Blocked requests

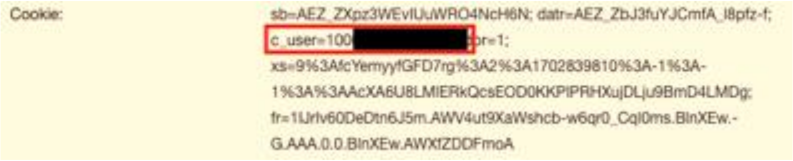
☐ 3rd-party requests

```
Name
fbevents.js
294530934476969?v=2.9.139&r=stable&dom...
569937663441474?v=2.9.139&r=stable&dom...
tr/?id=294530934476969&ev=PageView&dl=...
tr/?id=569937663441474&ev=PageView&dl=...
tr/?id=294530934476969&ev=Microdata&dl=...
tr/?id=569937663441474&ev=Microdata&dl=...
```

```
▾ General
Request URL:                        https://www.facebook.com/tr/?id=569937663441474&ev=PageView&dl=https%
                                    3A%2F%2Fwww.piedmont.org%2F&rl=https%3A%2F%2Fwww.piedmont.or
                                    g%2F&if=false&ts=1704817003633&sw=5120&sh=1440&v=2.9.139&r=stable&e
                                    c=0&o=4126&fbp=fb.1.1704581669191.1097695302&it=1704817003307&coo=f
                                    alse&rqm=GET
Request Method:                     GET
Status Code:                        ● 200 OK
Remote Address:                     157.240.19.35:443
Referrer Policy:                    strict-origin-when-cross-origin

▾ Response Headers
Access-Control-Allow-Credentials:   true
Access-Control-Allow-Origin:
Alt-Svc:                            h3=":443"; ma=86400
Content-Length:                     0
Content-Type:                       text/plain
Cross-Origin-Resource-Policy:       cross-origin
Date:                               Tue, 09 Jan 2024 16:16:43 GMT
Server:                             proxygen-bolt
Strict-Transport-Security:          max-age=31536000; includeSubDomains

▾ Request Headers
:authority:                         www.facebook.com
:method:                            GET
:path:                              /tr/?
                                    id=569937663441474&ev=PageView&dl=https%3A%2F%2Fwww.piedmont.o
                                    rg%2F&rl=https%3A%2F%2Fwww.piedmont.org%2F&if=false&ts=17048170
                                    03633&sw=5120&sh=1440&v=2.9.139&r=stable&ec=0&o=4126&fbp=fb.1.170
                                    4581669191.1097695302&it=1704817003307&coo=false&rqm=GET
:scheme:                            https
Accept:                             image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:                    gzip, deflate, br
Accept-Language:                    en-US,en;q=0.9
Cache-Control:                      no-cache
Cookie:                             sb=AEZ_ZXpz3WEvIUuWRO4NcH6N; datr=AEZ_ZbJ3fuYJCmfA_I8pfz-f;
                                    c_user=100[redacted]pr=1;
                                    xs=9%3AfcYemyyfGFD7rg%3A2%3A1702839810%3A-1%3A-
                                    1%3A%3AAcXA6U8LMIERkQcsEOD0KKPIPRHXujDLju9BmD4LMDg;
                                    fr=1IJrlv60DeDtn6J5m.AWV4ut9XaWshcb-w6qr0_Cql0ms.BlnXEw.-
                                    G.AAA.0.0.BlnXEw.AWXfZDDFmoA
```



```
Cookie:                             sb=AEZ_ZXpz3WEvIUuWRO4NcH6N; datr=AEZ_ZbJ3fuYJCmfA_I8pfz-f;
                                    c_user=100[redacted]pr=1;
                                    xs=9%3AfcYemyyfGFD7rg%3A2%3A1702839810%3A-1%3A-
                                    1%3A%3AAcXA6U8LMIERkQcsEOD0KKPIPRHXujDLju9BmD4LMDg;
                                    fr=1IJrlv60DeDtn6J5m.AWV4ut9XaWshcb-w6qr0_Cql0ms.BlnXEw.-
                                    G.AAA.0.0.BlnXEw.AWXfZDDFmoA
```

137. Therefore, Facebook could connect the cookie data that Piedmont transmitted with specified Users.

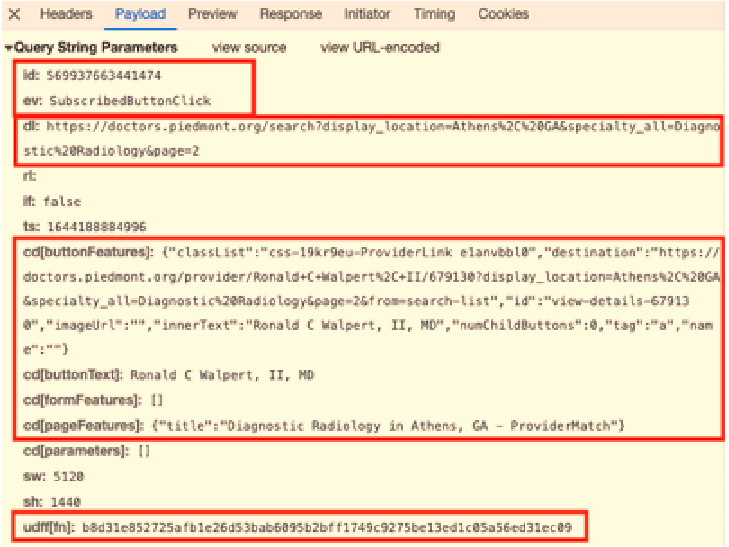
Piedmont Disclosed Users' Physician Search Activities

138. Upon a User's click to find doctors, Piedmont sent a SubscribedButtonClick event informing Facebook that the User clicked to "Find Doctors" at "Piedmont Healthcare | 16 Hospitals and Over 600 Locations." Piedmont then sent a set of PageView and Microdata events when the User loaded the page on https://doctors.piedmont.org/.

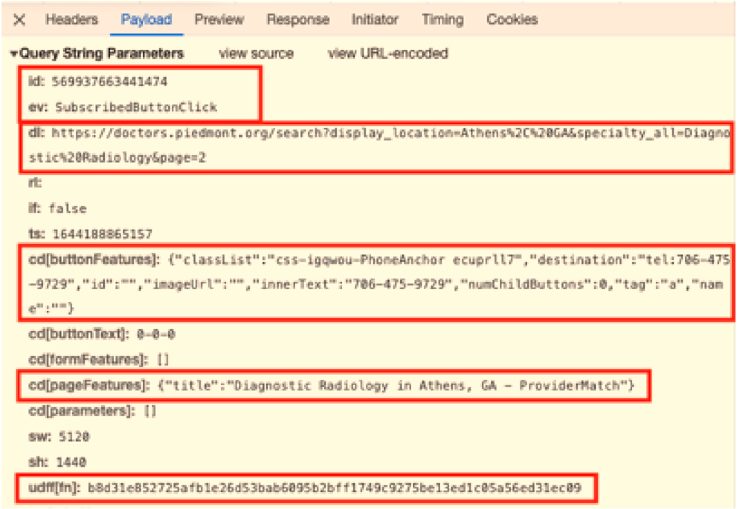
139. From the Find a Doctor page, the User may search for a doctor by adding parameters such as location and specialty. Piedmont also sent Facebook such user parameters. As an example, when a user searched for a provider near Athens with a specialty of diagnostic radiology, Piedmont sent PageView and Microdata events which reveal that the user sought a "ProviderMatch" for "Diagnostic Radiology in Athens, GA."

140. Piedmont then discloses the User's activities as they interact with their search results. For instance, the User could click to view a physician's page, call a physician, or book an appointment. As the User clicked for each action, Piedmont sent a SubscribedButtonClick event revealing the User's action and the context of the User's search for providers with a specialty of diagnostic radiology in Athens, Georgia.

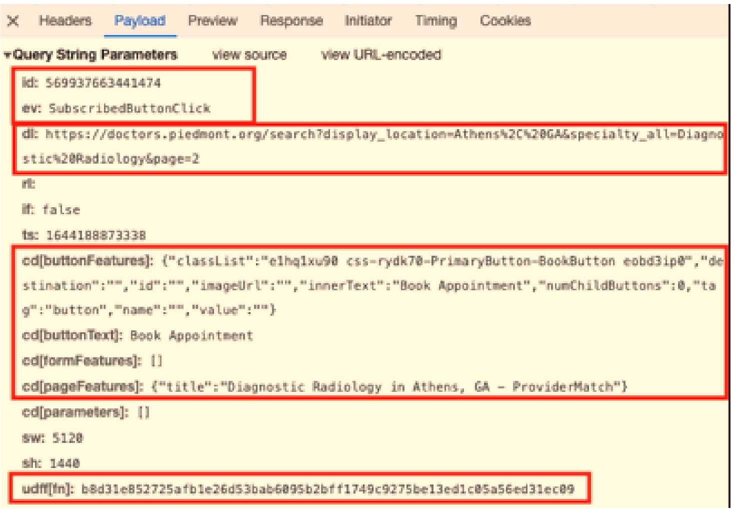
141. Specifically, when the User clicked to view a physician's profile, the SubscribedButtonClick event Piedmont sent states the name of the provider, for example, "Ronald C Walpert, II, MD." Similarly, Piedmont informed Facebook the precise phone number that the User clicked to call, "tel: 706-475-9729." And when the User clicked to book an appointment, Piedmont informed Facebook that the User clicked to "Book Appointment":



```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://doctors.piedmont.org/search?display_location=Athens%2C%20GA&specialty_all=Diagno
stic%20Radiology&page=2
rl:
if: false
ts: 1644188884996
cd[buttonFeatures]: {"classList":"css-19kr9eu-ProviderLink e1anvbbl0","destination":"https://
doctors.piedmont.org/provider/Ronald+C+Walpert%2C+II/679130?display_location=Athens%2C%20GA
&specialty_all=Diagnostic%20Radiology&page=2&from=search-list","id":"view-details-67913
0","imageUrl":"","innerText":"Ronald C Walpert, II, MD","numChildButtons":0,"tag":"a","nam
e":""}
cd[buttonText]: Ronald C Walpert, II, MD
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Diagnostic Radiology in Athens, GA - ProviderMatch"}
cd[parameters]: []
sw: 5120
sh: 1440
udff[fn]: b8d31e852725afb1e26d53bab6095b2bff1749c9275be13ed1c05a56ed31ec09
```



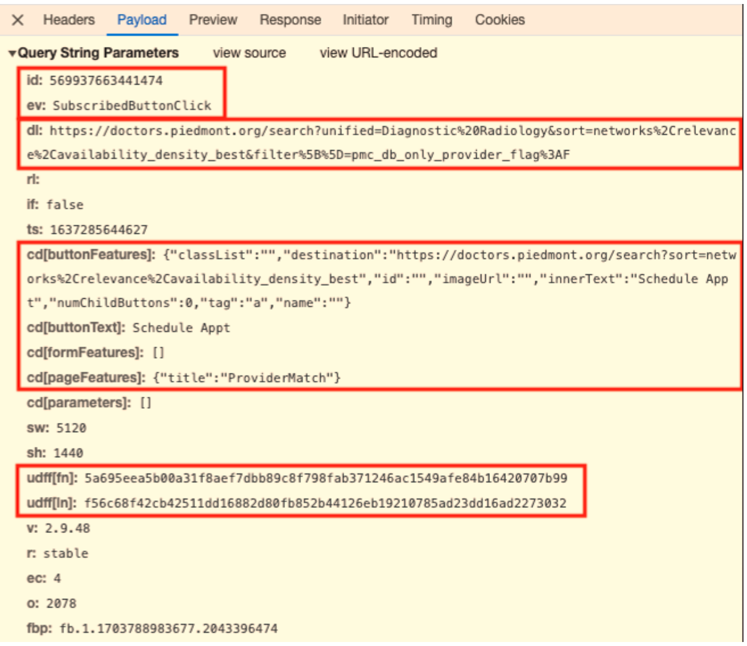
```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://doctors.piedmont.org/search?display_location=Athens%2C%20GA&specialty_all=Diagno
stic%20Radiology&page=2
rl:
if: false
ts: 1644188865157
cd[buttonFeatures]: {"classList":"css-igqwou-PhoneAnchor ecuprll7","destination":"tel:706-475
-9729","id":"","imageUrl":"","innerText":"706-475-9729","numChildButtons":0,"tag":"a","nam
e":""}
cd[buttonText]: 0-0-0
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Diagnostic Radiology in Athens, GA - ProviderMatch"}
cd[parameters]: []
sw: 5120
sh: 1440
udff[fn]: b8d31e852725afb1e26d53bab6095b2bff1749c9275be13ed1c05a56ed31ec09
```



```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://doctors.piedmont.org/search?display_location=Athens%2C%20GA&specialty_all=Diagno
stic%20Radiology&page=2
rl:
if: false
ts: 1644188873338
cd[buttonFeatures]: {"classList":"e1hq1xu90 css-rydk70-PrimaryButton-BookButton eobd3ip0","de
stination":"","id":"","imageUrl":"","innerText":"Book Appointment","numChildButtons":0,"ta
g":"button","name":"","value":""}
cd[buttonText]: Book Appointment
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Diagnostic Radiology in Athens, GA - ProviderMatch"}
cd[parameters]: []
sw: 5120
sh: 1440
udff[fn]: b8d31e852725afb1e26d53bab6095b2bff1749c9275be13ed1c05a56ed31ec09
```

142. Importantly, the SubscribedButtonClick events shown in the three figures above include the "udff[fn]" parameter, illustrating that Piedmont enabled **Advanced Matching Parameters**, which allow "Meta to connect collected event data to users, even if they do not have Facebook's browser cookies."[49] As illustrated in the figure below, both the "udff[fn]" and "udff[ln]" parameters were ultimately transmitted to Meta, which included both the first and the last name of the User:

[49] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector#advanced-matching-parameters.



```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://doctors.piedmont.org/search?unified=Diagnostic%20Radiology&sort=networks%2Crelevanc
e%2Cavailability_density_best&filter%5B%5D=pmc_db_only_provider_flag%3AF
rl:
if: false
ts: 1637285644627
cd[buttonFeatures]: {"classList":"","destination":"https://doctors.piedmont.org/search?sort=netw
orks%2Crelevance%2Cavailability_density_best","id":"","imageUrl":"","innerText":"Schedule App
t","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]: Schedule Appt
cd[formFeatures]: []
cd[pageFeatures]: {"title":"ProviderMatch"}
cd[parameters]: []
sw: 5120
sh: 1440
udff[fn]: 5a695eea5b00a31f8aef7dbb89c8f798fab371246ac1549afe84b16420707b99
udff[ln]: f56c68f42cb42511dd16882d80fb852b44126eb19210785ad23dd16ad2273032
v: 2.9.48
r: stable
ec: 4
o: 2078
fbp: fb.1.1703788983677.2043396474
```

Piedmont Disclosed Users' Keyword Search Activities

143. Mirroring Piedmont's disclosures about Piedmont's physician search activities, Piedmont also shared information with Facebook about Users' physician search activities.

144. When a User searched for the keyword, cancer, for example, Piedmont reported that through PageView and Microdata events which included the User's "query=cancer."

145. Users could refine their keyword search results by filtering based on whether the result is for Piedmont's services, facilities, or doctors. Piedmont reported as Users filtered their results.

146. For example, when the User filtered their cancer search results to show only Piedmont's offered services, Piedmont sent a SubscribedButtonClick event. The event informs Facebook that the User clicked on "Services" on a search results page for "query=cancer."

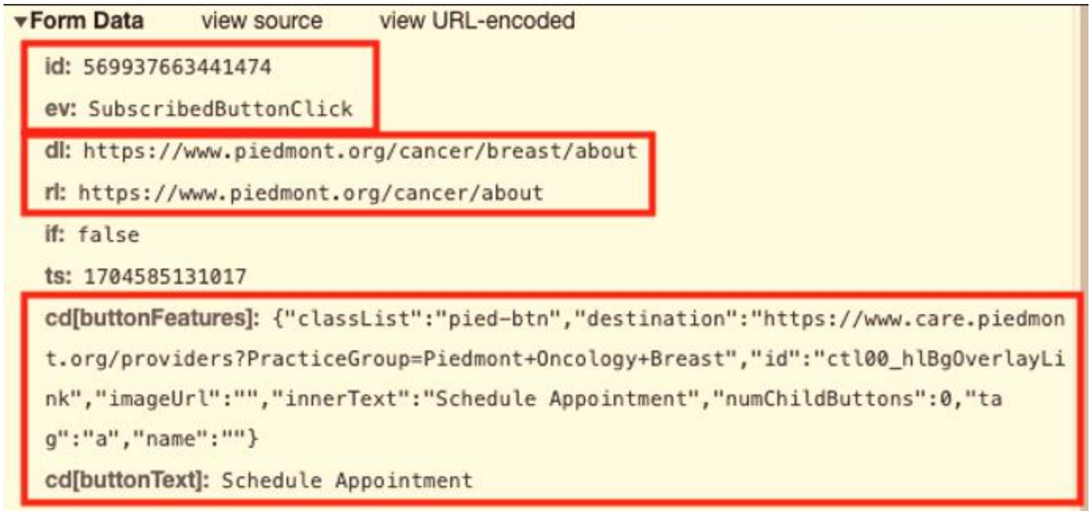
147. The User could then browse and click through their filtered search results to learn more and conduct activities such as book appointments. Piedmont disclosed details as Users performed these actions.

148. For instance, when the User clicked to view more about Piedmont's cancer services, and then clicked to open a page about breast cancer, Piedmont sent a series of SubscribedButtonClick, PageView, and Microdata events with details about the User's activities.

149. First, Piedmont transmitted SubscribedButtonClick, Pageview, and Microdata events disclosing that the User clicked to open a page about Piedmont's cancer care services after conducting a query for cancer. Then, as the User navigated to learn about breast cancer services, Piedmont informed Facebook through PageView and Microdata events that the User navigated from a page about cancer to a page about "cancer/breast."

Piedmont Disclosed Users' Appointment Activities

150. Continuing the example immediately above, where a User conducted a search for cancer and then proceeded to learn about breast cancer, when the User clicked to schedule an appointment, Piedmont transmitted a SubscribedButtonClick event:



```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://www.piedmont.org/cancer/breast/about
rl: https://www.piedmont.org/cancer/about
if: false
ts: 1704585131017
cd[buttonFeatures]: {"classList":"pied-btn","destination":"https://www.care.piedmon
t.org/providers?PracticeGroup=Piedmont+Oncology+Breast","id":"ctl00_hlBgOverlayLi
nk","imageUrl":"","innerText":"Schedule Appointment","numChildButtons":0,"ta
g":"a","name":""}
cd[buttonText]: Schedule Appointment
```

151. This event informs Facebook that the User clicked to "Schedule Appointment" which leads to "*https://www.care.piedmont.org/providers?Practicegroup=Peidmont+Oncology+Breast*."

152. Piedmont also offered a more generalized appointment booking function on its website. Piedmont informed Facebook about Users' appointment activities there as well.

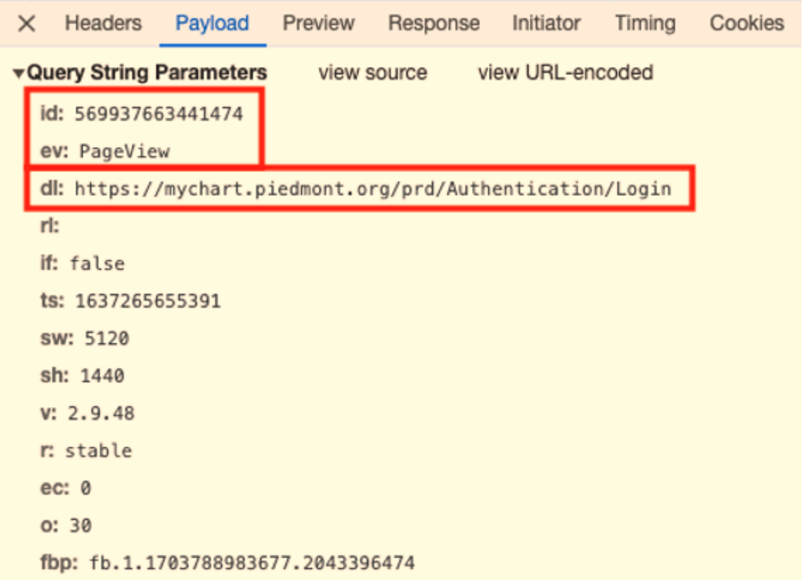
153. When a User clicked to "Schedule Appt" on Piedmont's website, Piedmont sent a SubscribedButtonClick event divulging to Facebook that the User clicked "Book Online."

154. Piedmont then sent PageView and Microdata events confirming the User loaded the Schedule Appointment page. Once the User was on the Schedule Appointment page, Piedmont populated the page with a list of locations with which and physicians with whom the User can book an appointment. When the User clicked "Book Appointment," and then "Book Online," Piedmont transmitted a SubscribedButtonClick event for each action disclosing the User's activities.

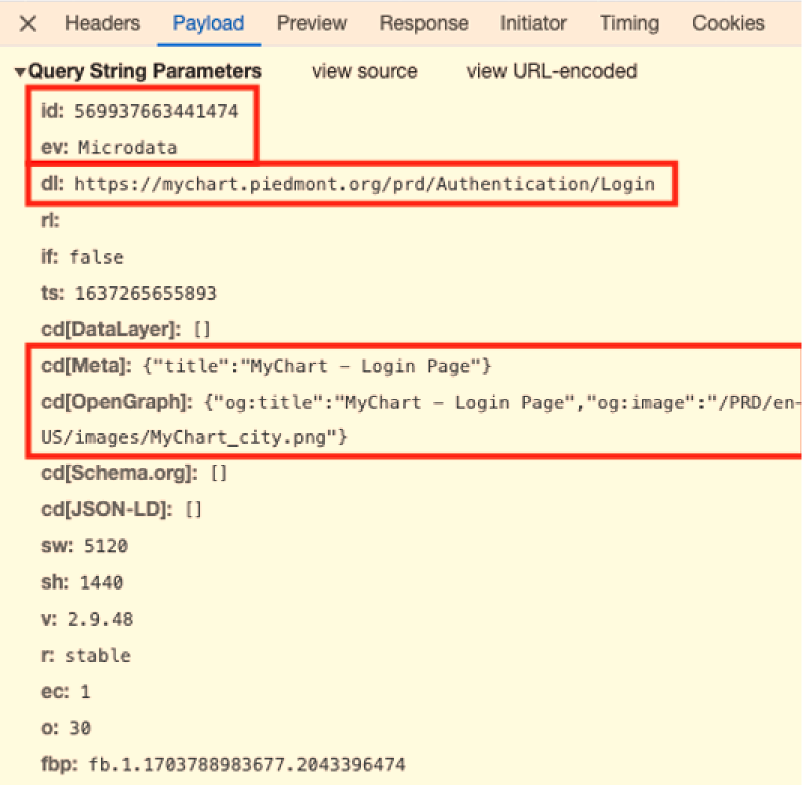
Piedmont Disclosed Users' MyChart Activities and Bill Pay Activities

155. Piedmont also disclosed User activities that reveal their status as current patients. Two examples of such activities are Users' MyChart and bill pay activities.

156. Upon a User's loading of the MyChart page, Piedmont informed Facebook that the User was on the page, "https://mychart.piedmont.org/prd/Authentication/Login." Importantly, this shows that Piedmont installed its Meta Pixels directly on its MyChart patient portal login page:



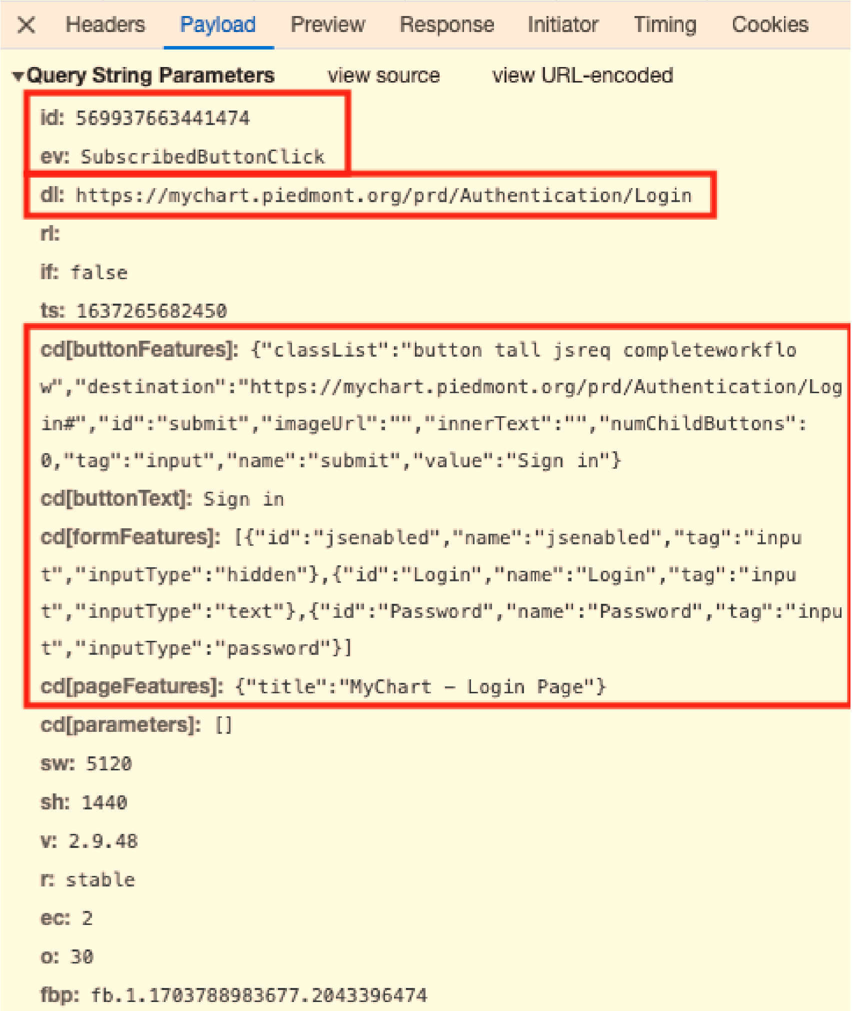
```
▾Query String Parameters
  id: 569937663441474
  ev: PageView
  dl: https://mychart.piedmont.org/prd/Authentication/Login
  rl:
  if: false
  ts: 1637265655391
  sw: 5120
  sh: 1440
  v: 2.9.48
  r: stable
  ec: 0
  o: 30
  fbp: fb.1.1703788983677.2043396474
```



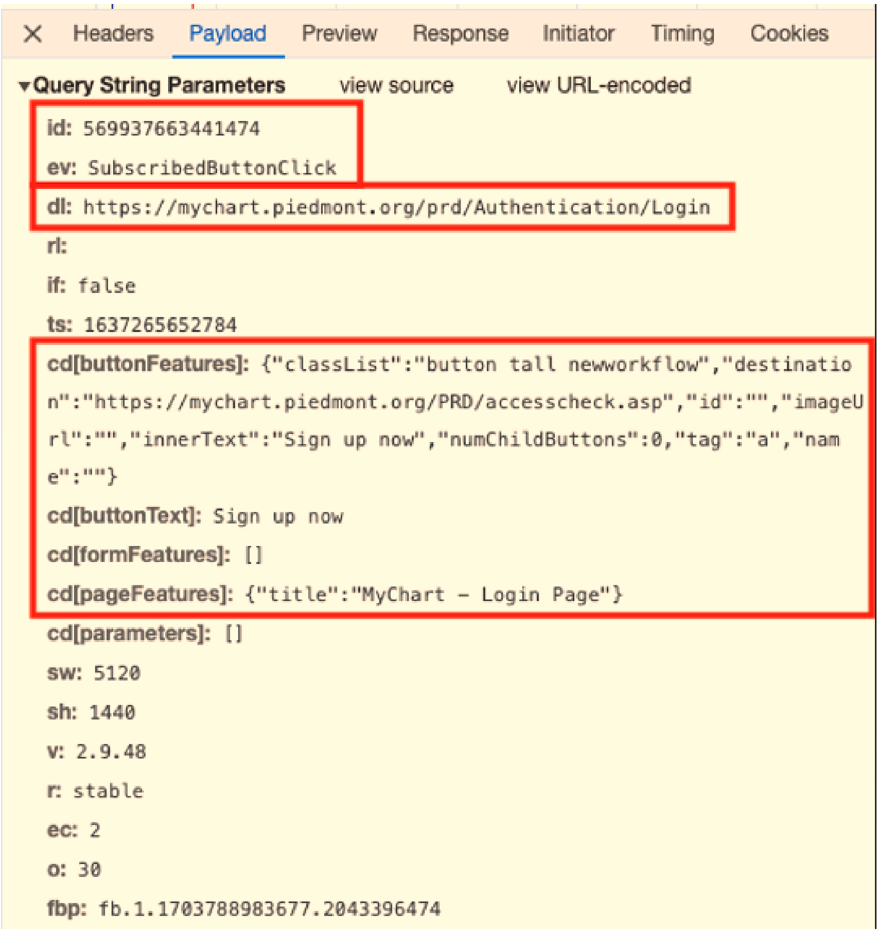
```
▾Query String Parameters
  id: 569937663441474
  ev: Microdata
  dl: https://mychart.piedmont.org/prd/Authentication/Login
  rl:
  if: false
  ts: 1637265655893
  cd[DataLayer]: []
  cd[Meta]: {"title":"MyChart - Login Page"}
  cd[OpenGraph]: {"og:title":"MyChart - Login Page","og:image":"/PRD/en-
  US/images/MyChart_city.png"}
  cd[Schema.org]: []
  cd[JSON-LD]: []
  sw: 5120
  sh: 1440
  v: 2.9.48
  r: stable
  ec: 1
  o: 30
  fbp: fb.1.1703788983677.2043396474
```

157. From the MyChart page, the User could either click to sign into or sign up for a MyChart account. When the User did either, Piedmont sent a

SubscribedButtonClick event informing Facebook that the User either clicked to "Sign in" or clicked to "Sign up now" on the "MyChart – Login Page":



```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://mychart.piedmont.org/prd/Authentication/Login
rl:
if: false
ts: 1637265682450
cd[buttonFeatures]: {"classList":"button tall jsreq completeworkflo
w","destination":"https://mychart.piedmont.org/prd/Authentication/Log
in#","id":"submit","imageUrl":"","innerText":"","numChildButtons":
0,"tag":"input","name":"submit","value":"Sign in"}
cd[buttonText]: Sign in
cd[formFeatures]: [{"id":"jsenabled","name":"jsenabled","tag":"inpu
t","inputType":"hidden"},{"id":"Login","name":"Login","tag":"inpu
t","inputType":"text"},{"id":"Password","name":"Password","tag":"inpu
t","inputType":"password"}]
cd[pageFeatures]: {"title":"MyChart – Login Page"}
cd[parameters]: []
sw: 5120
sh: 1440
v: 2.9.48
r: stable
ec: 2
o: 30
fbp: fb.1.1703788983677.2043396474
```



```
id: 569937663441474
ev: SubscribedButtonClick
dl: https://mychart.piedmont.org/prd/Authentication/Login
rl:
if: false
ts: 1637265652784
cd[buttonFeatures]: {"classList":"button tall newworkflow","destination":"https://mychart.piedmont.org/PRD/accesscheck.asp","id":"","imageUrl":"","innerText":"Sign up now","numChildButtons":0,"tag":"a","name":""}
cd[buttonText]: Sign up now
cd[formFeatures]: []
cd[pageFeatures]: {"title":"MyChart - Login Page"}
cd[parameters]: []
sw: 5120
sh: 1440
v: 2.9.48
r: stable
ec: 2
o: 30
fbp: fb.1.1703788983677.2043396474
```

158. Similarly, when a User clicked to access the Pay Your Bill page, Piedmont informed Facebook that the User clicked “Pay Bill” to navigate to https://www.piedmont.org/patient-tools/bill-pay.

159. Subsequently, Piedmont transmitted PageView and Microdata events, confirming the User arrived on the page to “Pay Your Bill | Piedmont Healthcare.”

160. If the User had questions about their bills, they could contact Piedmont. When the User clicked to email Piedmont, Piedmont informed Facebook about this through a SubscribedButtonClick event.

161. The event reveals that the User clicked to email "mailto:customerservice@piedmont.org" on the "Pay Your Bill | Piedmont Healthcare" page.

F. Piedmont's Privacy Policies & Promises.

162. Defendant's privacy policies represent to Plaintiffs and Class Members that Defendant will keep Private Information private and confidential, and it will only disclose Private Information under certain circumstances.

163. Defendant publishes several privacy policies that represent to Users that Piedmont will keep sensitive information confidential and that it will only disclose PII and PHI provided to it under certain circumstances, none of which apply here.[50]

164. Defendant's separate Notice of Privacy Practices assures Plaintiffs and Class Members that Piedmont is "committed to keeping your health information private."[51]

[50] https://www.piedmont.org/about-piedmont-healthcare/joint-notices/privacy-policy (last visited Jan. 12, 2024).

[51] https://www.piedmont.org/media/file/PHC-Joint-Notice-Privacy-Practice.pdf (last visited Jan. 10, 2024).

165. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to PHI and the exceptions for when Defendant can lawfully use and disclose Plaintiffs' and Class Members' PHI in the following ways:

- For Treatment;
- For Payment;
- For Health Care Operations;
- For Medical Research;
- As Required by Law and Law Enforcement;
- For Public Health Activity;
- For Health Oversight Activities;
- Organ, Eye and Tissue Donation;
- Coroners, Medical Examiners, Funeral Directors and Individuals Involved in Your Health Care or Payment for Your Health Care;
- Uses and Disclosures for Involvement in Your Care;
- To Avoid a Serious Threat to Health or Safety or in Disaster Relief Efforts;
- Specialized Government Functions;
- Workers' Compensation;

- Fundraising Efforts;
- Appointment Reminders, Follow-Up Care and Treatment Alternatives;
- Patient Directories.[52]

166. Defendant also promises patients that "[o]ther types of uses and disclosures of your PHI not described in this Notice will be made only with your written authorization."[53]

167. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiffs' and Class Members' PHI for marketing purposes contrary to law, stating that it may "not use and disclose [Plaintiffs' or Class Members'] PHI for marketing purposes except in limited circumstances as authorized by law or unless [Plaintiffs' or Class Members'] have given us written authorization."[54]

168. Notwithstanding these representations, Piedmont designed the Meta Collection Tools it used to capture both the "characteristics" of individual patients' communications with Piedmont's Web Properties (i.e., their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of

[52] *Id.*

[53] *Id.*

[54] *Id.*

these communications (i.e., the URLs, buttons, links, pages, and tabs they click and view).

169. Piedmont installed Meta’s Collection Tools on its Web Properties and, thereafter, began to automatically transmit extensive individually identifiable patient health information from everyone who visited its Web Properties to Meta.

170. After receiving individually identifiable health information communicated on Piedmont’s Web Properties, Meta analyzes and uses this information for its own commercial purposes that include building more fulsome profiles of its Users’ preferences and traits and selling targeted advertisements based on this information. Meta also receives an additional commercial benefit from Piedmont’s use of Meta’s Collection Tools, namely that it provides Piedmont with a greater incentive to advertise on Meta’s social media platforms.

171. After receiving individually identifiable patient health information communicated on Piedmont’s Web Properties, Meta forwards this data, and its analysis of this data, to Piedmont. Piedmont then uses this data and analysis for its own commercial purposes that include understanding how people use its Website and determining what ads people see on its Website.

172. Meta is not an intended recipient of the individually identifiable health information communicated by patients on Piedmont’s Web Properties, nor is it an

active or disclosed participant in these communications. However, Piedmont intended for Meta to be the intended recipient of patient communications containing individually identifiable health information.

173. At all times relevant to this Complaint, Piedmont did not notify Users that it automatically sends individually identifiable health information communicated on its Web Properties to Meta.

174. At all times relevant to this Complaint, Piedmont did not notify Users of its Web Properties that individually identifiable health information they communicate on its Web Properties were being used by Meta for commercial purposes.

175. At all times relevant to this Complaint, Piedmont did not notify Users of its Web Properties that it was using the individually identifiable health information they communicate on its Web Properties for commercial purposes.

176. Meta has not secured any informed consent or written permission allowing it to use individually identifiable health information communicated on Piedmont's Web Properties for commercial purposes.

177. Piedmont has not secured any informed consent or written permission allowing it to share individually identifiable health information communicated on its Web Properties with Meta.

178. Piedmont has not secured any informed consent or written permission allowing it to use individually identifiable health information communicated on its Web Properties for commercial purposes.

179. Piedmont violated its own privacy policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

G. Meta Falsely Promises Facebook Users That It Requires Healthcare Partners to Have the Right to Share Their Data.

180. Every Facebook user is legally deemed to have agreed to the Terms of Service, Data Policy/Privacy Policy, and Cookie Policy via a checkbox on the sign-up page. The Terms of Service, Data Policy/Privacy Policy, and Cookie Policy are binding on Meta and its users.

181. The Meta contract documents contain general statements that, in exchange for the use of Meta's services, Meta will generally collect information about Facebook users.

182. Meta does not charge users any money to use its services, but Meta is not "free."

183. In 2019, Meta removed language on its webpage that stated, "It's free and always will be."[55] This conduct demonstrates that using Meta is not, in fact, free. As a digital law expert has explained: "Facebook is not free nor has it ever been. Facebook's currency was and still is its users' personal data. It's never been free, though, because data is worth a lot of money." *Id.*

184. Rather than making users pay money out-of-pocket to use Facebook, Meta makes them pay for its services by allowing Meta to collect some types of personal data under a "data license."

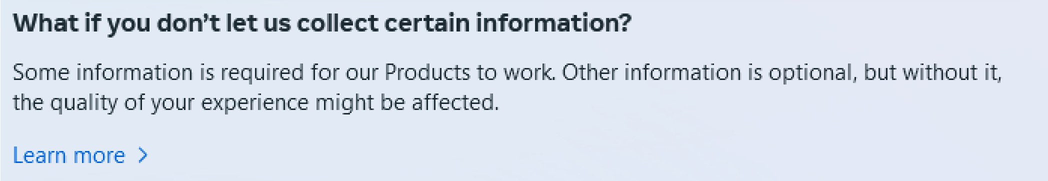
185. Meta's contract states, "We collect and use your personal data in order to provide the services described above to you." It then informs users, "You can learn how we collect and use your data in our Data Policy."[56]

186. Although the Meta Data Policy makes general broad disclosures about the data it collects, the scope of Meta's "data license" is not unlimited. For example, by signing up for Meta, a Facebook user has not agreed to exchange with Meta the right for Meta to obtain their bank account information or Social Security number.

[55]https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8.

[56] The hyperlink to Data Policy sends users to the Meta Privacy Policy at https://www.facebook. com/privacy/policy/?entry point=data policy redirect&entry=0.

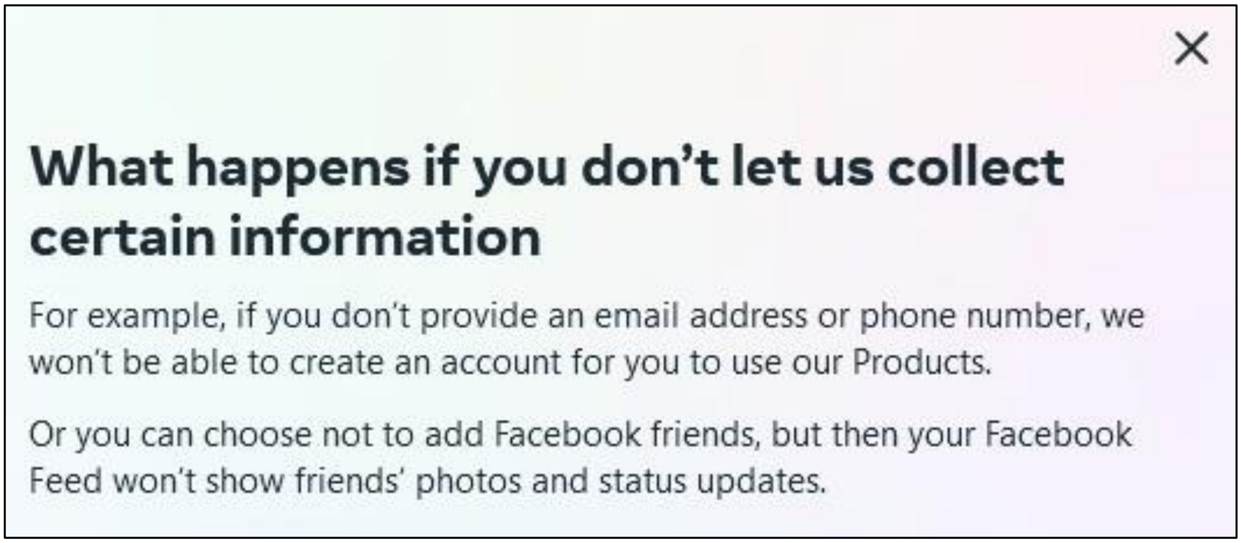
Instead, the Meta Privacy Policy establishes a minimum amount of information users must provide directly to Meta to use Meta's products:



What if you don't let us collect certain information?

Some information is required for our Products to work. Other information is optional, but without it, the quality of your experience might be affected.

187. When a Facebook user clicks the "Learn more" hyperlink to learn what "information is required" for Facebook to work, Meta provides examples of how choosing not to share information will prevent users from creating a Facebook account or using its features:



What happens if you don't let us collect certain information

For example, if you don't provide an email address or phone number, we won't be able to create an account for you to use our Products.

Or you can choose not to add Facebook friends, but then your Facebook Feed won't show friends' photos and status updates.

188. Meta's Terms of Service also expressly incorporates the Meta Privacy Policy by hyperlink, stating that "Our Privacy Policy explains how we collect and

use your personal data to determine some of the ads you see and provide all of the other services described" in Meta's Terms of Service.

189. The Meta Privacy Policy has a section titled "What information do we collect?" in which Meta tells users:

> Meta, we use information to provide you with a more personal, secure, and meaningful experience. But where does that information come from? The information we collect comes from a variety of sources.... *And, sometimes businesses also share information with us like your activity on their websites. They may also share experiences you have offline, like signing up for a Rewards card with your email address*. This makes it easier for them to share promotions, product information, and other ads with you through our ads consistent with the choices that you make.[57]

190. The Meta Privacy Policy does not state that Meta actively solicits Facebook users' healthcare providers, health insurers, pharmacies, prescription drug companies, and other covered entities under 45 C.F.R. § 160.103 to become Meta Partners using Meta's business services.

191. The Meta Privacy Policy does not state that, in exchange for use of its Products, Meta will collect health information from a Facebook user's healthcare providers, health insurers, pharmacies, prescription drug companies, or other

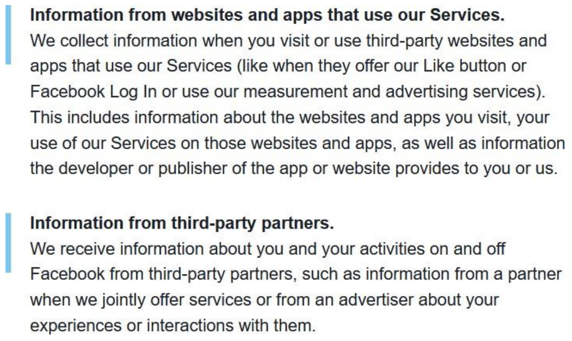
[57] *Id*. (emphasis added).

covered entities under 45 C.F.R § 160.103 about the Facebook user, including their communications, actions, and status as patients with those health entities.

192. In addition to not obtaining specific consent, Meta affirmatively promises users that it requires "Partners" to have the right to share the users' data before providing it to Meta.

193. Before April 2018, Meta's contract did not require Partners to have the lawful right to share user data before doing so:

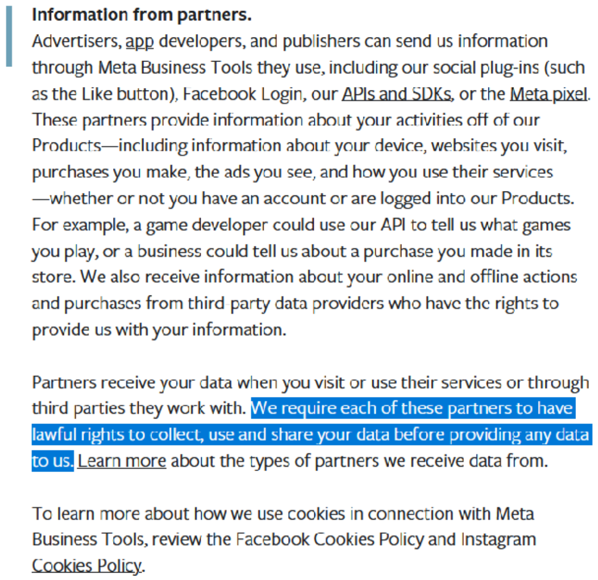
Before April 19, 2018



Information from websites and apps that use our Services.
We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

Information from third-party partners.
We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

After April 19, 2018



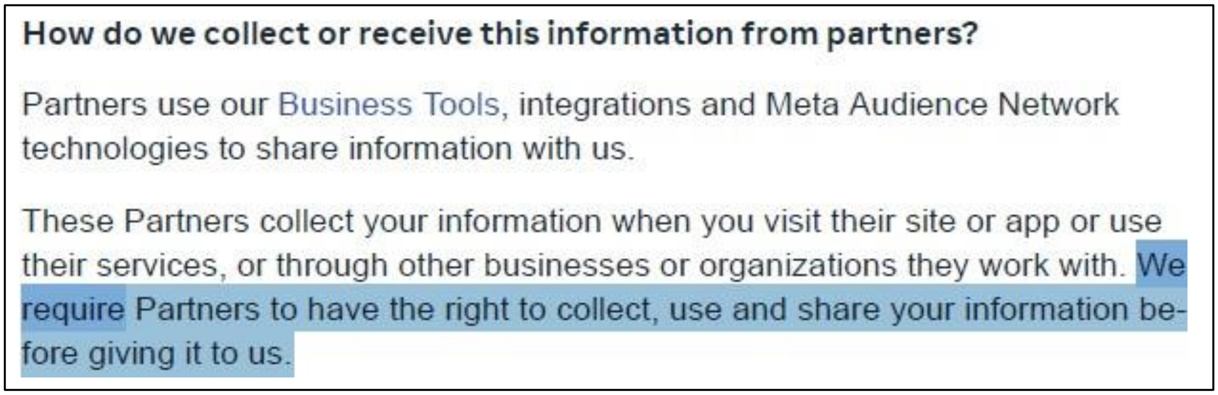
Information from partners.
Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.

To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

194. Meta changed this provision again in July 2022 to remove the word "lawful" while still promising that it requires partners to have the right to share patient information with Meta:[58]

195. Meta does not verify that healthcare providers or covered entities have provided adequate notice and obtained valid consent or authorization to share their patients' data with Meta.[59]



How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

196. Meta's contract with healthcare providers for use of the Meta Pixel does not mention HIPAA.

[58] Meta, Data Policy: Information from Partners, vendors and third parties (Jan. 1, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartners Vendors.

[59] The European Union recently ruled that Meta's attempt to obtain consent from users by including a clause in its terms and conditions allowing Meta to collect their data for personal advertising violated Europe's General Data Protection Regulation. Adam Satariano, *Meta's Ad Practices Ruled Illegal Under E.U. Law*, N.Y. Times (Jan. 4, 2023), *https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html.*

197. Meta does not use an advanced technical system to monitor whether Meta Collection Tools are installed on websites that will transmit individually identifiable health information to Meta. To the contrary, Meta Health urges healthcare providers and other covered entities to use Meta Collection Tools to target ads to patients.

198. Meta maintains a "Health" marketing division called Meta Health, with a page at *https://www.facebook.com/business/industries/consumer-goods/healthcare* where Meta offers advertisers the chance to "get help growing your healthcare business" and explains how "Healthcare marketers are partnering with Meta."

199. Meta Health is dedicated to helping web developers and advertisers in healthcare related industries to increase their marketing spend with Meta and improve their marketing campaigns using Meta Collection Tools.

200. Meta Health's role is to "inform" healthcare marketers "to think about how we can really disrupt health and how we market to patients."[60]

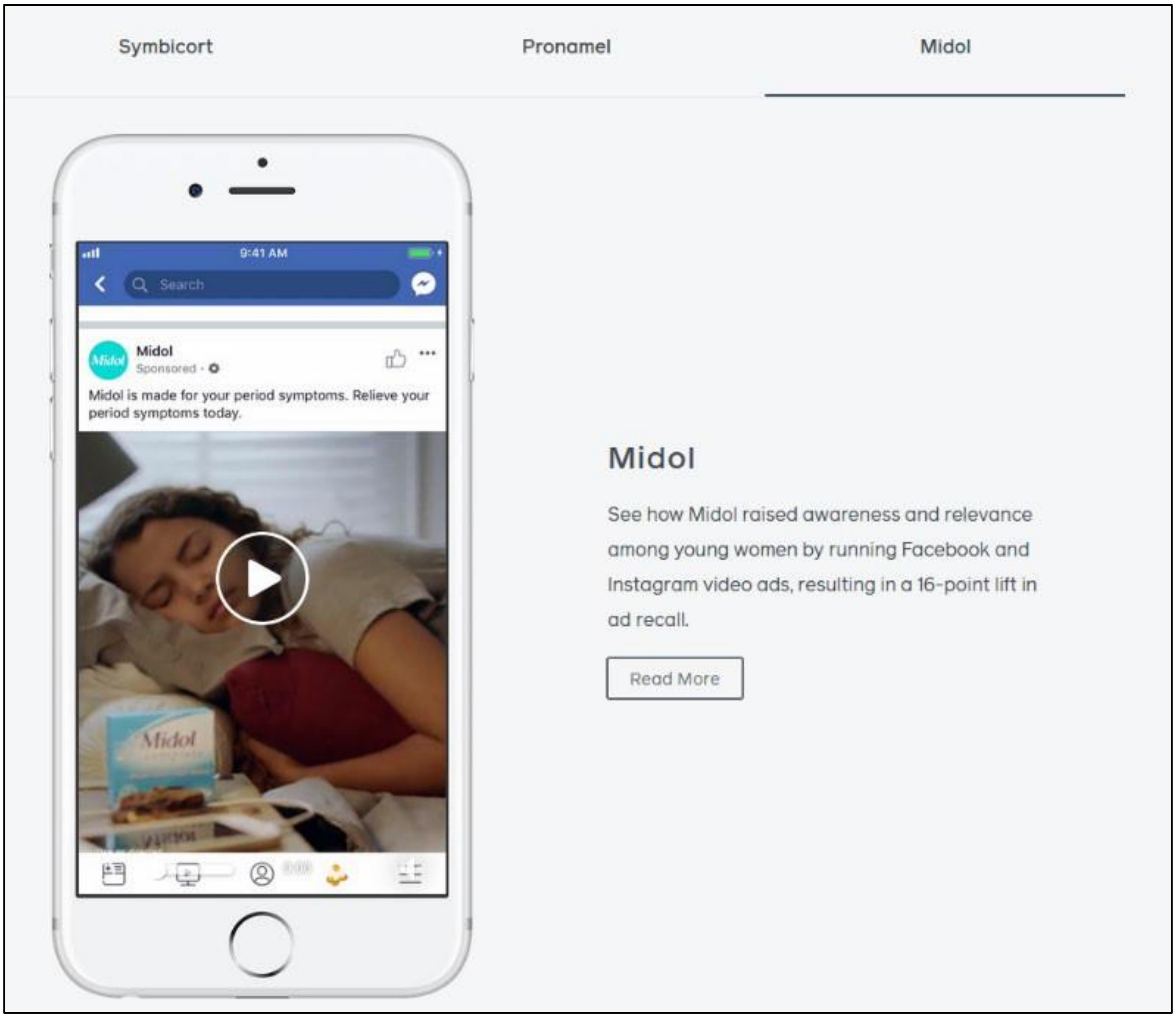
[60] Facebook Disrupting Health: A Conversation with Jasson Gilmore, *https://www.facebook.com /business/industries/health?deeplink=829704181304626*.

201. Meta Health employees are assigned to specific healthcare providers and other covered entities to encourage and aid their use of Meta Collection Tools for targeting patients.

202. Meta provides guidance and resources for web developers and advertisers on a dedicated webpage at *https://www.facebook.com/business/industries/health*. Among other things, this webpage includes examples of advertising campaigns so that web developers and advertisers can "See how health brands are reaching new audiences with Facebook advertising."

203. For example, Meta highlights an advertising campaign aimed at "young women" through video ads promising to "Relieve your period symptoms today." [61]

[61] *Midol* (2023), https://www.facebook.com/business/success/2-midol.



Midol is made for your period symptoms. Relieve your period symptoms today.

Midol

See how Midol raised awareness and relevance among young women by running Facebook and Instagram video ads, resulting in a 16-point lift in ad recall.

204. Meta has also engaged in similar advertising campaigns relating to treatments for acne, allergies, arthritis, birth control, diabetes, erectile dysfunction, hair loss, high cholesterol, migraines, and many more prescription drugs and treatments.[62]

[62] *See generally* Meta, Get winning advertising solutions from businesses like yours (2023), *https://www.facebook.com/business/success/categories/health-pharmaceuticals*. The "marketing case studies" on this page change on occasion.

DEFENDANT'S CONDUCT VIOLATES FEDERAL & STATE PRIVACY LAWS

A. The HIPAA Privacy Rule Protects Patient Healthcare Information

205. Patient healthcare information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

206. The HIPAA Privacy Rule, located at 45 C.F.R. § 160 and 45 C.F.R. § 164 (A) and (E): "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.[63]

207. The Privacy Rule broadly defines PHI as "individually identifiable health information" ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

[63] HHS.gov, *Health Information Privacy* (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

208. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

209. Under the HIPAA de-identification rule, "health information is not individually-identifiable only if: (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

a. Names;

b. Medical record numbers;

c. Account numbers;

> d. Device identifiers and serial numbers;
>
> e. Web Universal Resource Locators (URLs);
>
> f. Internet Protocol (IP) address numbers; … and
>
> g. Any other unique identifying number, characteristic, or code…; and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information." 45 C.F.R. § 164.514.

210. The HIPAA Privacy Rule requires any "covered entity"—which includes healthcare providers like Piedmont—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

211. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually-identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually-identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

212. The criminal and civil penalties imposed by 42 U.S.C. § 1320(d)(6) apply directly to Piedmont when it is knowingly disclosing IIHI relating to an individual, as those terms are defined under HIPAA.

213. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains IIHI relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

B. HIPAA Protects Patient Status Information

214. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.

215. Guidance from HHS confirms that HIPAA protects patient status:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.… **If such information was listed with health condition, healthcare provision or payment data, such as an indication that an individual was treated at a certain**

> **clinic, then this information would be PHI.**[64]

216. HHS's guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, **covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list**.[65]

217. HHS has previously instructed that the HIPAA Privacy Rule protects patient status:

[64] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[65] Office for Civil Rights, *Marketing* at 1-2 (emphasis added) (Apr. 3, 2003), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.*

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

C. HIPAA's Protections Do Not Exclude Internet Marketing

218. In December 2022, HHS issued a bulletin "to highlight the obligations" of healthcare providers and their business associates under the HIPAA Privacy Rule "when using online tracking technologies" such as the "Meta Pixel," which "collect

and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[66]

219. In this bulletin, HHS confirmed that HIPAA applies to healthcare providers' use of tracking technologies like the Meta Pixel.[67] Among other things, HHS explained that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually-identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of

[66] HHS.gov, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information* (Dec. 1, 2022), *https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requir ements-under-hipaa-for-online-tracking-technologies.html.*

[67] HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa- online-tracking/index.html.*

> appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of healthcare services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care**.[68]

220. HHS explained that tracking technologies on healthcare providers' patient portals "generally have access to PHI" and may access diagnosis and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user- authenticate webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. **Tracking**

[68] *Id.*

> **technologies within user- authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal**. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[69]

221. HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal:

Tracking on unauthenticated webpages

> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … **[and pages] that address[] specific symptoms or health conditions,** such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering **credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search

[69] *Id.*

> for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[70]

222. As a result, a healthcare provider may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI. If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization. [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a

[70] *Id.*

> signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.[71]

223. HHS's bulletin did not create any new obligations. Instead, it merely highlighted long-standing obligations based on previous guidance and rules that have been in place for decades.

D. Under HIPAA, IP Addresses are Personally Identifiable Information.

224. Through the use of the Meta Pixel, computer IP addresses are among the Private Information that was improperly disclosed to Facebook.

225. An IP address is a number that identifies the address of a device connected to the Internet.

226. IP addresses are used to identify and route communications on the Internet.

227. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

228. Facebook tracks every IP address ever associated with a Facebook user.

229. Google also tracks IP addresses associated with Internet users.

[71] *Id.*

230. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

231. Under HIPAA, an IP address is considered personally identifiable information:

> a. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
>
> b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

232. Consequently, by disclosing Plaintiffs' and Class Members' IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

E. The FTC Act Protects Health Information.

233. The FTC has made clear that "health information" is "anything that conveys information—or enables an information—about a consumer's health" and provides an example that location-data alone (such as repeated trips to a cancer

treatment facility") "may convey highly sensitive information about a consumer's health."[72]

234. The FTC joined HHS in notifying HIPAA-covered entities and non-HIPAA-covered entities that sharing such "health information" with Google and Facebook is an unfair business practice under federal law:

> When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."[73]

[72] Jillson, Elisa, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, Federal Trade Commission (July 25, 2023), *https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases*.

[73] *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, Federal Trade Commission (July 20, 2023), *https:// www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking*.

F. Georgia Law Protects Health Information.

235. O.C.G.A. § 31-33-2 states that providers, which are defined to include hospitals, O.C.G.A. § 31-33-1, may only release medical records "upon written request from the patient or a person authorized to have access to the patient's record under an advance directive for health care, a psychiatric advance directive, or a durable power of attorney for health care for such patient," where "the record request [is] accompanied by: [a]n authorization in compliance with the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Section 1320d-2, et seq., and regulations implementing such act" and "a signed written authorization indicating that he or she is authorized to have access to the patient's records[.]"."

236. In addition, O.C.G.A. § 31-33-8 provides that health records in electronic format are "subject to all applicable federal laws governing the security and confidentiality of a patient's personal health information."

237. Thus, Georgia law requires all hospitals, including Piedmont, to maintain all medical records and information within their control as confidential, rendering Piedmont's actions with respect to the interception and disclosure of its patients' Private Information to Meta unlawful under Georgia law.

G. Piedmont Violated Industry Standards.

238. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship, it is a cardinal rule.

239. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

240. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

241. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-

> making capacity about the purposes for which access would be granted.

242. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

H. Plaintiffs' & Class Members' Expectations of Privacy

243. Plaintiffs and Class Members were aware of Piedmont's duty of confidentiality when they sought medical services from Piedmont.

244. Indeed, at all times when Plaintiffs and Class Members provided their PII and PHI to Piedmont, they each had a reasonable expectation that the information would remain private and that Piedmont would not share their Private Information with third parties for a commercial purpose, unrelated to patient care.

245. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

246. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe

those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[74]

247. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

248. Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' Private Information, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

[74] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), available at https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Jan. 9, 2024).

I. Patients Have Protectable Property Interests in Their IIHI.

249. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiffs and the Class members have a vested property right in their IIHI.

250. Federal and state laws grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

251. A patient's right to protect the confidentiality of their health data and restrict access to this data is valuable.

252. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA. State health privacy laws and American courts have also long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

253. Property rights in communications and information privacy are established by:

a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored

Communications Act); and Title III (the Pen Register Act); and

b. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, s*ee Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

254. Meta's CEO, Mark Zuckerberg, has acknowledged that Meta users have an ownership interest in their data. In 2010, when Meta first revealed its "Download Your Information" tool, Zuckerberg stated that, "People own and have control over all info they put into Facebook and 'Download Your Information' enables people to take stuff with them."[75] Although Zuckerberg's statements regarding people's ability to "control" the information "put into Facebook" and the ability to access all such data via DYI is not true, his statement about data ownership is true.

255. Piedmont's unauthorized interception and disclosure of Plaintiffs' and the Class members' individually identifiable health information violated their property rights to control how their data and communications are used and who may be the beneficiaries of their data and communications.

[75] https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/.

J. The Information Piedmont Discloses to Meta Without Plaintiffs' or Class Members' Consent Has Actual, Measurable Monetary Value.

256. After receiving individually identifiable patient health information communicated on Piedmont's Web Properties, Facebook forwards this data, and its analysis of this data, to Piedmont.

257. Piedmont then uses this data and analysis for its own commercial purposes that include understanding how Users utilize its Web Properties.

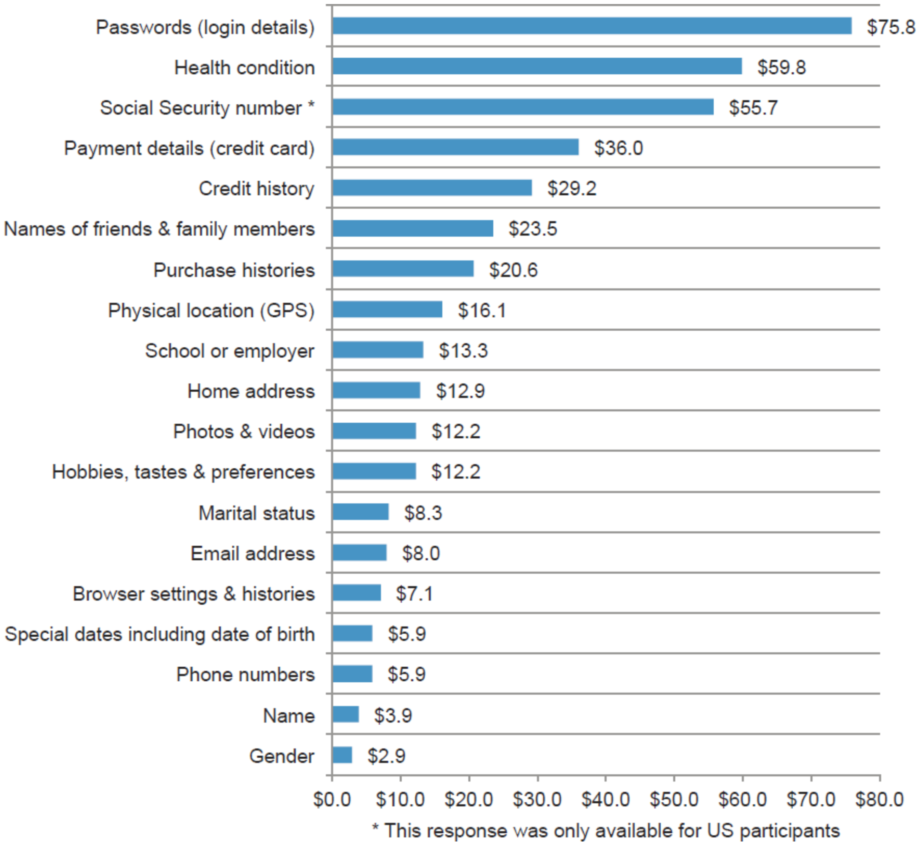
258. Technology companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

259. Meta "generate[s] substantially all of [its] revenue from advertising."[76]

260. Meta annually receives billions of dollars of unearned advertising sales revenue from Meta healthcare Partners, including Piedmont, who are targeting Facebook users based on their health information.

[76] Meta 2022 Annual Report at 17.

261. The data that Meta collects without authorization has monetary value. For example, a 2015 study found respondents placed a value of $59.80 on an individual's health information:



262. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[77] A 2015 article from TechCrunch accurately noted that "[d]ata

[77] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Jan. 9, 2024).

has become a strategic asset that allows companies to acquire or maintain a competitive edge."[78]

263. That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

264. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[79] That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

265. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[80]

[78] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Jan. 9, 2024).

[79] *See What Your Data is Really Worth to Facebook* (Jul. 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ (last visited Jan. 9, 2024).

[80] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

266. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[81]

267. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

268. Courts recognize the value of personal information and the harm when it is disclosed without consent. See, e.g., In re Facebook Privacy Litig., 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

[81] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Jan. 9, 2024).

269. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

270. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

271. The value of health data is well-known and various reports have been conducted to identify its value.

272. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[82]

[82] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Jan. 9, 2024).

273. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[83]

274. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[84]

275. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[85]

[83] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Jan. 9, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[84] *See* https://time.com/4588104/medical-data-industry/ (last visited Jan. 9, 2024).

[85] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Jan. 9, 2024).

276. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

277. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

278. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

K. Defendant was Enriched & Benefitted from the Use of The Meta Pixel & Unauthorized Disclosures.

279. The sole purpose of the Meta Pixel on Defendant's Web Properties was marketing and revenue.

280. In exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

281. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and

cookies to track website visitors and then places ads on other websites the visitor goes to later.[86]

282. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a healthcare website back to Facebook via the tracking technologies and the Meta Pixel embedded on, in this case, Piedmont's Web Properties. For example, when a User searches for doctors or medical conditions or treatment on Piedmont's Web Properties, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a Piedmont ad and ensure that those Users targeted are more likely to convert.[87]

283. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[88]

[86] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Jan. 9, 2024).

[87] *See, e.g., How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), *https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking* (last visited Jan. 9, 2024).

[88] *Id.*

284. Plaintiffs' and Class Members' Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

285. In exchange for disclosing the Private Information of their account holders and patients, Piedmont is compensated in the form of enhanced advertising services and more cost-efficient marketing on its platform.

286. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[89]

287. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you

[89] *See The guide to HIPAA compliance in analytics*, https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Jan. 9, 2024).

followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[90]

288. Meta's Terms of Service, Data Policy, and Cookies Policy neither inform Facebook users that Meta may acquire their health information when they interact with healthcare providers' websites and applications, nor obtain their consent for any such acquisitions.

289. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[91]

290. Whether a User has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the Meta Pixel's ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

[90] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra*, n.87.

[91] *The complex world of healthcare retargeting*, *supra*, n.86.

291. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients connected to the Piedmont MyChart portal.

292. By utilizing the Meta Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

<u>REPRESENTATIVE PLAINTIFFS' EXPERIENCES</u>

A. Plaintiff T.D.'s Experience

293. Plaintiff T.D. entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff T.D. disclosed his Private Information to Defendant.

294. On numerous occasions, from 2016 to present, Plaintiff T.D. accessed mychart.piedmont.org and Defendant's Website on his mobile device and/or computer to receive healthcare services from Defendant and at Defendant's direction.

295. Plaintiff T.D. used Defendant's Web Properties to look for health care providers and to schedule doctor's appointments for himself, including an annual physical.

296. For example, in October 2021 Plaintiff T.D. used Defendant's MyChart to make a doctor's appointment that he attended in November 2021.

297. Plaintiff T.D. has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

298. Plaintiff T.D. provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

299. Plaintiff T.D. reasonably expected that his communications with Defendant via the Web Properties were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

300. Pursuant to the systematic process described herein, Piedmont assisted Facebook with intercepting Plaintiff T.D.'s communications, including those that contained personally identifiable information, protected health information, and related confidential information.

301. Defendant transmitted to Facebook Plaintiff T.D.'s Facebook ID, computer IP address; and information such as his medical conditions, treatments sought, appointment type and date, and physician selected.

302. Piedmont assisted these interceptions without Plaintiff T.D.'s knowledge, consent, or express written authorization. By failing to receive the

requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff T.D.'s personally identifiable information and protected health information.

303. Defendant did not inform Plaintiffs T.D. that it had shared his Private Information with Facebook.

304. Plaintiff T.D. is diagnosed with a specific medical condition and submitted information to Defendant's website about scheduling medical appointments for his medical condition to Facebook.

305. Plaintiff T.D. suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to his Private Information.

306. Plaintiff T.D. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure.

B. Plaintiff A.G.'s Experience

307. Plaintiff A.G. entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff A.G. disclosed his Private Information to Defendant.

308. On numerous occasions, from at least 2021 to present, Plaintiff A.G. accessed mychart.piedmont.org and Defendant's Website on his mobile device and/or computer to receive healthcare services from Defendant and at Defendant's direction.

309. Plaintiff A.G. used Defendant's Web Properties to look for health care providers and to schedule doctor's appointments for himself, including an annual physical.

310. For example, in 2021 and continuing through May 2022, Plaintiff A.G. used Defendant's MyChart to schedule approximately five doctor's appointments that he attended.

311. Plaintiff A.G. has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

312. Plaintiff A.G. provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

313. Plaintiff A.G. reasonably expected that his communications with Defendant via the Web Properties were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted

by a third party.

314. Pursuant to the systematic process described herein, Piedmont assisted Facebook with intercepting Plaintiff A.G.'s communications, including those that contained personally identifiable information, protected health information, and related confidential information.

315. Defendant transmitted to Facebook Plaintiff A.G.'s name, Facebook user ID, and information such as his appointment type, appointment date and time, and physician selected.

316. Piedmont assisted these interceptions without Plaintiff A.G.'s knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff A.G.'s personally identifiable information and protected health information.

317. Defendant did not inform Plaintiff A.G. that it had shared his Private Information with Facebook.

318. Plaintiff A.G. is diagnosed with a specific medical condition and submitted information to Defendant's website about scheduling medical appointments for his medical condition to Facebook.

319. Plaintiff A.G. suffered damages in the form of (i) invasion of privacy;

(ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

320. Plaintiff A.G. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure.

C. Plaintiff J.G.'s Experience

321. Plaintiff J.G. entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff J.G. disclosed her Private Information to Defendant.

322. On numerous occasions, from at least 2018 to present, Plaintiff J.G. accessed mychart.piedmont.org and Defendant's Website on her mobile device and/or computer to receive healthcare services from Defendant and at Defendant's direction.

323. Plaintiff J.G. used Defendant's Web Properties to look for health care providers and to schedule doctor's appointments for herself.

324. For example, in 2018 and continuing through May 2022, Plaintiff J.G. used Defendant's MyChart to schedule approximately four doctor's appointments

that she attended, including appointments on July 26, 2019, June 22, 2020, May 12, 2021, and May 12, 2022 for annual physicals and to discuss mental health diagnoses and treatments.

325. Plaintiff J.G. has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

326. Plaintiff J.G. provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

327. Plaintiff J.G. reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

328. Pursuant to the systematic process described herein, Piedmont assisted Facebook with intercepting Plaintiff J.G.'s communications, including those that contained personally identifiable information, protected health information, and related confidential information.

329. Defendant transmitted to Facebook Plaintiff J.G.'s name, Facebook user ID, and information such as her appointment type, appointment date and time, and physician selected.

330. Piedmont assisted these interceptions without Plaintiff J.G.'s knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff J.G.'s personally identifiable information and protected health information.

331. Defendant did not inform Plaintiff J.G. that it had shared her Private Information with Facebook.

332. Plaintiff J.G. is diagnosed with a specific medical condition and submitted information to Defendant's website about scheduling medical appointments for her medical condition to Facebook.

333. After communicating Private Information on Piedmont's Web Properties, including MyChart, she began regularly receiving healthcare-related ads on Facebook, including for Teledoc, throughout approximately 2021 to 2023.

334. Plaintiff J.G. suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

335. Plaintiff J.G. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's

possession, is protected and safeguarded from future unauthorized disclosure.

D. Plaintiff K.W.'s Experience

336. Plaintiff K.W. entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff K.W. disclosed his Private Information to Defendant.

337. On numerous occasions, from at least 2020 to present, Plaintiff K.W. accessed mychart.piedmont.org and Defendant's Website on his mobile device and/or computer to receive healthcare services from Defendant and at Defendant's direction.

338. Plaintiff K.W. used Defendant's Web Properties to look for health care providers and to schedule doctor's appointments for himself including for digestive health issues and x-ray imaging.

339. For example, throughout 2020, 2021, and 2022, Plaintiff K.W. used Defendant's MyChart to schedule approximately nine doctor's appointments that he attended, including appointments on June 15, 2020; October 7, 2020; December 31, 2020; January 26, 2021; March 2, 2021; March 2, 2021; April 29, 2021; June 1, 2021; and August 22, 2022. K.W. also paid medical bills for numerous of these appointments using MyChart.

340. Plaintiff K.W. has used the same devices to maintain and access an

active Facebook account throughout the relevant period in this case.

341. Plaintiff K.W. provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

342. Plaintiff K.W. reasonably expected that his communications with Defendant via the Web Properties were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

343. Pursuant to the systematic process described herein, Piedmont assisted Facebook with intercepting Plaintiff K.W.'s communications, including those that contained personally identifiable information, protected health information, and related confidential information.

344. Defendant transmitted to Facebook Plaintiff K.W.'s name, Facebook user ID, and information such as his appointment type, appointment date and time, and physician selected.

345. Piedmont assisted these interceptions without Plaintiff K.W.'s knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff K.W.'s personally identifiable information and protected health

information.

346. Defendant did not inform Plaintiff K.W. that it had shared his Private Information with Facebook.

347. Plaintiff K.W. is diagnosed with a specific medical condition and submitted information to Defendant's website about scheduling medical appointments for his medical condition to Facebook.

348. Plaintiff K.W. suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

349. Plaintiff K.W. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure.

TOLLING

350. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its incorporation of the Meta Pixel into its Web Properties.

351. The Meta Pixel and other tracking tools on Defendant's Web Properties were and are entirely invisible to a Web Properties visitor.

352. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

353. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

354. Defendant had exclusive knowledge that its Web Properties incorporated the Meta Pixel and other tracking tools and yet failed to disclose to its patients, including Plaintiffs and Class Members, that by seeking medical care through Defendant's Website, Plaintiffs' and Class Members' Private Information would be disclosed or released to Facebook and other unauthorized third parties.

355. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its patients' Private Information. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise indicated to its patients that it has disclosed or released their Private Information to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

356. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

357. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of the original complaint in this suit.

CLASS ACTION ALLEGATIONS

358. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Fed. R. Civ. P. 23.

359. The Class that Plaintiffs seek to represent is defined as follows:

> All persons residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Collection Tools on Defendant's Web Properties.

360. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

361. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

362. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The Class members are so numerous that joinder of all members is impracticable. Upon information and belief,

there are millions of individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant's records.

363. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant violated its Privacy Policies by disclosing the Private Information of Plaintiffs and Class Members to Facebook and/or additional third parties;

d. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policy practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of Defendant's disclosure of their Private Information.

364. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Meta Pixel, due to Defendant's misfeasance.

365. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully disclosed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on

Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

366. **<u>Adequacy of Representation</u>, Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

367. **<u>Superiority and Manageability</u>, Fed. R. Civ. P. 23(b)(3):** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large

corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

368. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

369. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is

representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

370. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

371. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

372. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

373. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

374. Likewise, particular issues under Fed.R.Civ.P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CLAIMS FOR RELIEF

COUNT I

INVASION OF PRIVACY—
INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs & the Class)

375. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

376. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

377. Defendant owed a duty to Plaintiffs and Class Members to keep their PII and PHI confidential.

378. The unauthorized disclosure and/or acquisition by a third party of Plaintiffs' and Class Members' PII and PHI is highly offensive to a reasonable person.

379. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' PII and PHI constitutes an intentional interference with Plaintiffs' and the

Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

380. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

381. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted with a knowing state of mind when it incorporated the Meta Pixel into its website because it knew the functionality and purpose of the Meta Pixel.

382. Because Defendant intentionally and willfully incorporated the Meta Pixel into its Web Properties and encouraged patients to use those Web Properties for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members.

383. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiffs and the Class Members was disclosed to a third party without authorization, causing Plaintiffs and the Class to suffer damages.

384. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

385. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

386. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, who on information and belief continues to possess and utilize that information.

387. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II

BREACH OF FIDUCIARY DUTY
(*On Behalf of Plaintiffs & the Class*)

388. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

389. In light of the special relationship between Defendant Piedmont and Plaintiffs and Class Members, whereby Defendant Piedmont became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant Piedmont did and does store.

390. Defendant Piedmont has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant Piedmont's relationship with its patients and former patients, in particular, to keep secure their Private Information.

391. Defendant Piedmont breached its fiduciary duties to Plaintiffs and Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiffs and Class Members of this fact.

392. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members.

393. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

394. As a direct and proximate result of Defendant Piedmont's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of ill-gotten gains, in an amount to be proven at trial.

COUNT III

NEGLIGENCE (INCLUDING NEGLIGENCE PER SE)
(On Behalf of Plaintiffs & the Class)

395. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

396. Defendant Piedmont required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare services.

397. Upon accepting, storing, and controlling the Private Information of Plaintiffs and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

398. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

399. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information through its use of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook, gaining access to such Private Information for no lawful purpose.

400. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class Members' Private Information arose due to the special relationship that existed between Defendant and its patients, which is recognized by statute, regulations, and the common law.

401. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients'

healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

402. Defendant Piedmont's duty to use reasonable security measures under HIPAA required Defendant Piedmont to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

403. In addition, Defendant Piedmont had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

404. Defendant Piedmont's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described

above, but also because Defendant is bound by industry standards to protect confidential Private Information.

405. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information.

406. Defendant's misconduct included the failure to (1) secure Plaintiffs' and Class Members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixels and other tracking technologies; and (5) prevent unauthorized access to Plaintiffs' and Class Members' Private Information by sharing that information with Facebook and other third parties. Defendant's failures and breaches of these duties constituted negligence.

407. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' Private Information, Plaintiffs and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

408. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class members' Private Information constituted (and continue to constitute) negligence at common law.

409. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiffs and Class Members are entitled to recover those damages in an amount to be determined at trial.

410. Defendant Piedmont's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant Piedmont to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiffs' and Class Members' Private Information with Facebook and other third parties without Plaintiffs' and Class Members' express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

<u>COUNT IV</u>

BREACH OF IMPLIED CONTRACT

<u>(On behalf of Plaintiffs & the Class)</u>

411. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

412. When Plaintiffs and Class Members provided their user data to Defendant Piedmont in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

413. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

414. Plaintiffs and Class Members would not have entrusted Defendant Piedmont with their Private Information in the absence of an implied contract between them and Defendant Piedmont obligating Defendant not to disclose this Private Information without consent.

415. Defendant Piedmont breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to a third party, *i.e.*, Facebook.

416. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged

herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

417. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V

BREACH OF CONTRACT
(On behalf of Plaintiffs and the Class)

418. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

419. Plaintiffs and Class Members allege they entered into valid and enforceable express contracts, or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

420. Specifically, Plaintiffs and Class Members entered into a valid and enforceable express contract with Defendants when Plaintiffs first received medical care from Defendant.

421. The valid and enforceable express contracts to provide medical and health care services that Plaintiffs and Class Members entered into with Defendant

include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

422. Under these express contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

423. Both the provision of medical services and the protection of Plaintiffs and Class Members' Private Information were material aspects of these express contracts.

424. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

425. At all relevant times, Defendant expressly represented in their Privacy Notice, among other things: (i) that Piedmont is "committed to keeping [Plaintiffs' and Class Members'] health information private"; (ii) that "uses and disclosures of [Plaintiffs' and Class Members'] PHI not described in this Notice will be made only

with [Plaintiffs' and Class Members'] written authorization"; and (iii) that it may "not use and disclose [Plaintiffs' or Class Members'] PHI for marketing purposes except in limited circumstances as authorized by law or unless [Plaintiffs' or Class Members'] have given us written authorization."[92]

426. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

427. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entered into these contracts with Defendant and/or their affiliated

[92] https://www.piedmont.org/media/file/PHC-Joint-Notice-Privacy-Practice.pdf (last visited Jan. 10, 2023).

healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

428. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

429. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

430. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

431. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Web

Properties. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class Members' Private Information, as set forth above.

432. The mass and systematic disclosure of Plaintiffs' and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

433. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

434. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

435. In addition, or in the alternative, Defendant breached the express contracts by breaching the implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms. In Georgia, a breach of contract claim may lie where the defendant acts in bad faith when exercising discretion over the performance of its duties under the contract.[93] Here, Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties and breached the implied covenant of good faith and fair dealing by presenting its healthcare services as private, secure, and in compliance with federal law, including HIPAA, while secretly, systematically, and repeatedly disclosing Private Information to Meta through the Meta Collection Tools, failing to disclose to Plaintiffs and Class Members that it disclosed Private Information to Meta through the Meta Collection Tools, and continuing to disclose Private Information to Meta through the Meta Collection Tools even after being called out in the media for its egregious acts—all in flagrant violation of the most publicly-known and sacrosanct provisions federal law: HIPAA.

[93] *See, e.g.*, *ULQ, LLC v. Meder*, 293 Ga. App. 176, 179, 666 S.E.2d 713, 717 (2008) ("where the manner of performance is left more or less to the discretion of one of the parties to the contract, he is bound to the exercise of good faith").

436. As a direct and proximate result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

437. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta.

COUNT VI
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

438. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the proposed Class.

439. This count is pled in the alternative to Plaintiffs' Breach of Implied Contract and Breach of Contract counts.

440. Defendant Piedmont benefits from Plaintiffs and Class Members and unjustly retained those benefits at their expense.

441. Plaintiffs and Class Members conferred a benefit upon Defendant Piedmont in the form of Private Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

442. That is, in exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook. By utilizing the Meta Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

443. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

444. The benefits that Defendant Piedmont derived from Plaintiffs and Class Members were not offered by Plaintiffs and Class Member gratuitously and rightly

belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in Georgia for Defendant to be permitted to retain any of the revenue or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

445. Defendant Piedmont should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VII

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use and Disclosure
(*On Behalf of Plaintiffs and the Class*)

446. Plaintiffs repeat the allegations contained in the foregoing paragraphs preceding this Counts Section as if fully set forth herein and bring this claim individually and on behalf of the Class.

447. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

448. The ECPA protects both the sending and receipt of communications.

449. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

450. Piedmont intentionally intercepted electronic communications that Plaintiffs and the Class members exchanged with Piedmont through the Meta Collection Tools installed on Piedmont's Web Properties.

451. The transmissions of data between Plaintiffs and the Class members and Piedmont qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

452. Piedmont contemporaneously intercepted and transmitted Plaintiffs' and the Class members' communications to Meta.

453. The intercepted communications include:

a. the content of Plaintiffs' and the Class members' registrations for the Patient Portal, including clicks on buttons to "Register" or "Signup" for portals;

b. the content Plaintiffs' and the Class members' log in and log out of the Patient Portal, including clicks to "Sign-in," or "Log-in";

c. the content of communications that Plaintiffs and the Class members exchange inside the Patient Portal immediately before logging out of the portal, specifically including the act of paying medical bills;

d. the content of Plaintiffs' and the Class members' communications relating to appointments with medical providers;

e. upon information and belief, the content of Plaintiffs' and the Class members' communications relating to specific healthcare providers, conditions, treatments, diagnoses, prognoses, prescription drugs, symptoms, insurance, and payment information; and

f. Full-string URLs that contain any information concerning the substance, purport, or meaning of patient communications with their health entities.

454. For example, Defendant's interception of the fact that a patient views a webpage like *"https://www.care.piedmont.org/providers?Practicegroup=Peidmont+Oncology+Breast"* involves "content," because it communicates that patient's request for the information on that page.

455. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. the cookies Piedmont and Meta use to track Plaintiffs' and the Class members' communications;

b. Plaintiffs' and the Class members' browsers;

c. Plaintiffs' and the Class members' computing devices;

d. Piedmont's web-servers or webpages where the Meta Collection Tools are present;

e. Meta's web-servers; and

f. the Meta Collection Tools source code Piedmont deploys on its Web Properties to acquire Plaintiffs' and the Class members' communications.

456. Meta is not a party to Plaintiffs' and the Class members' communications with Piedmont.

457. Piedmont transmits the content of Plaintiffs' and the Class members' communications to Meta through the surreptitious redirection of those communications from Plaintiffs' and the Class members' computing devices.

458. Plaintiffs and the Class members did not consent to Meta's acquisition of their patient portal, appointment, and treatment communications with Piedmont.

459. Meta did not obtain legal authorization to obtain Plaintiffs' and the Class members' communications with Piedmont relating to communications with their health entities.

460. Meta did not require Piedmont to obtain the lawful rights to share the content of Plaintiffs' and the Class members' communications relating to patient portals, appointments, and treatments.

461. Any purported consent that Meta received from Piedmont to obtain the content of Plaintiffs' and the Class members' communications was not valid.

462. In disclosing the content of Plaintiffs' and the Class members' communications relating to patient portals, treatments, conditions, and

appointments, Piedmont had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions including:

a. the unauthorized disclosure of individually identifiable health information is tortuous in and of itself regardless of whether the means deployed to disclose the information violates the Wiretap Act or any subsequent purpose or use for the acquisition. Piedmont intentionally committed a tortious act by disclosing individually identifiable health information without authorization to do so.

b. the unauthorized acquisition of individually identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually identifiable health information. Piedmont intentionally violated 42 U.S.C. 1320d-6 by intentionally disclosing individually identifiable health information without authorization.

c. a violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment with *increased penalties* where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain." Piedmont intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by disclosing the individually identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

d. a knowing intrusion upon Plaintiffs' and the Class members' seclusion;

e. trespass upon Plaintiffs' and the Class members' personal and private property via the placement of an _fbp cookie associated with Piedmont's Web Properties on Plaintiffs' and the Class members' personal computing devices;

f. the requirements under O.C.G.A. § 31-33-2 and O.C.G.A. § 31-33-8 that healthcare providers maintain the confidentiality of patient health records; and

g. violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy), which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

463. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that is was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. The attempt version of the wire fraud statute provides that "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 18 U.S.C. § 1349.

464. Piedmont's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the breach of contract and negligence claims below;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie of Piedmont's Web Properties rather than a third-party cookie from Meta.

465. Piedmont acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and the Class members' property:

a. property rights to the confidentiality of their individually identifiable health information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

466. Piedmont acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and the Class members' property:

a. with knowledge that (1) Piedmont did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their individually-identifiable health information based on their activities on

Piedmont's Web Properties; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of individually-identifiable health information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC; and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their individually-identifiable health information for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiffs' and the Class members' individually-identifiable health information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiffs' and the Class members' individually-identifiable health information without their authorization; and (3) gain access to the Plaintiffs' and the Class members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie.

467. Any purported consent provided by Piedmont using the Meta Collection Tools had a purpose that was tortious, criminal, and in violation of state constitutional and statutory provisions because it constitutes:

a. knowing intrusion into a private matter that would be highly offensive to a reasonable person;

b. a violation of 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment and that includes increased penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage [or] personal gain."

c. trespass;

d. breach of fiduciary duty; and

e. a violation of various state health privacy and computer privacy statutes, including the CCPA and the CIPA.

468. Plaintiffs and the Class members have suffered damages because of Piedmont’s violations of the ECPA that include:

a. Piedmont eroded the essential, confidential nature of the provider-patient relationship;

b. Piedmont failed to provide Plaintiffs and the Class members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;

c. Piedmont derived valuable benefits from using and sharing the contents of Plaintiffs’ and the Class members’ communications on its Web Properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. Piedmont’s actions deprived Plaintiffs and the Class members of the value of their individually identifiable health information;

e. Piedmont’s actions diminished the value of Plaintiffs’ and the Class Members’ property rights in their individually identifiable health information; and

f. violating Plaintiffs' and the Class members' privacy rights by sharing their individually identifiable health information for commercial use.

469. For Piedmont's violations set forth above, Plaintiffs and the Class members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Piedmont] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

470. Unless enjoined, Piedmont will continue to commit the violations of law alleged here.

471. Plaintiffs want to continue to communicate with their healthcare provider through online platforms but have no practical way of knowing if their communications are being intercepted and disclosed to Meta, and thus continue to be at risk of harm from Piedmont's conduct.

472. Pursuant to 18 U.S.C. § 2520, Plaintiffs and the Class members seek monetary damages for the *greater of* (i) the sum of the actual damages suffered by the plaintiff and any revenue made by Piedmont as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request judgment in their favor and against Defendant and that the Court grant the following:

A. an Order certifying the Class and appointing Plaintiffs and their Counsel to represent the Class;

B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. injunctive relief requested by Plaintiffs including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorneys' fees, costs, and litigation expenses, as allowed by law, including, but not limited to, O.C.G.A.

§ 13-6-11, due to Defendant's bad faith in deceitfully and purposefully procuring Plaintiffs' and Class Members' Private Information, payment, and other consideration with no intent to honor its promises to keep their Private Information confidential;

F. prejudgment interest on all amounts awarded; and

G. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: January 12, 2024

Respectfully Submitted,

PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP

By: */s/ Andrew R. Tate*
Andrew R. Tate
GA Bar # 518068
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Ph: 404-282-4806
atate@peifferwolf.com

/s/ Brandon M. Wise
Brandon M. Wise

IL Bar # 6319580*
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

ALMEIDA LAW GROUP LLC

/s/ David S. Almeida
David S. Almeida
NY Bar # 3056520*
Elena Belov
NY Bar # 4080891*
Britany Kabakov
IL Bar # 6336126*
849 W. Webster Avenue
Chicago, Illinois 60614
Ph: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com
britany@almeidalawgroup.com

**pro hac vice*

Counsel for Plaintiffs & the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of January 2024, I caused a true and correct copy of the foregoing motion to be filed with the Clerk of the Court via the Court’s CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matter.

PEIFFER WOLF CARR KANE CONWAY
& WISE, LLP

By: *<u>/s/ Andrew R. Tate</u>*

Counsel for Plaintiffs and the Proposed Class